

#2



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Shoji Goto et al.

Application No.: Unassigned

Filed: Herewith

For: A METHOD OF UPDATING
PROGRAM IN STORED CONTROL
PROGRAM UNIT AND A STORED
CONTROL PROGRAM UNIT

Examiner: Not Assigned

Art Unit: Not Assigned

SUBMISSION OF PRIORITY
DOCUMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Applicant respectfully submits priority document Japan P2000-159549 filed
May 25, 2000, to be made of record in the above-referenced application.

Respectfully submitted,

Robert C. Colwell
Reg. No. 27,431

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, 8th Floor
San Francisco, California 94111-3834
Tel.: (650) 326-2400
Fax: (650) 326-2422
RCC:KK:amc
PA 3125001 v1

Patent Office
Japanese Government



This is to certify that the annexed is a true copy of the following application as filed with this office.

Date of Application : May 25, 2000
Application Number: P2000-159549

Application (s): Hitachi, Ltd.
Hitachi Software Engineering Co., Ltd.

Dated this 6th day of October 2000

Kozo Oikawa
Patent Office

Certificate No. 2000-3081686

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2000年 5月25日

出 願 番 号

Application Number:

特願2000-159549

出 願 人

Applicant (s):

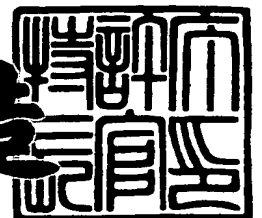
株式会社日立製作所

日立ソフトウェアエンジニアリング株式会社

2000年10月 6日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2000-3081686

【書類名】 特許願

【整理番号】 K00003541

【提出日】 平成12年 5月25日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 3/06
G06F 3/301

【請求項の数】 3

【発明者】

【住所又は居所】 神奈川県小田原市国府津 2 8 8 0 番地 株式会社日立製作所 ストレージシステム事業部内

【氏名】 後藤 昌治

【発明者】

【住所又は居所】 神奈川県小田原市国府津 2 8 8 0 番地 株式会社日立製作所 ストレージシステム事業部内

【氏名】 山本 政信

【発明者】

【住所又は居所】 東京都千代田区神田駿河台四丁目 6 番地 株式会社日立製作所内

【氏名】 木下 敏夫

【発明者】

【住所又は居所】 神奈川県横浜市中区尾上町 6 丁目 8 1 番地 日立ソフトウェアエンジニアリング株式会社内

【氏名】 小林 隆直

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社日立製作所

【特許出願人】

【識別番号】 000233055

【氏名又は名称】 日立ソフトウェアエンジニアリング株式会社

【代理人】

【識別番号】 100075096

【弁理士】

【氏名又は名称】 作田 康夫

【手数料の表示】

【予納台帳番号】 013088

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 制御プログラム内蔵型装置のプログラム更新方式及び制御プログラム内蔵型装置

【特許請求の範囲】

【請求項 1】

制御プログラム内蔵型装置と、前記制御プログラム内蔵型装置の制御プログラム原本の保管と配信を行う制御プログラム配信装置と、前記制御プログラム内蔵型装置の制御プログラムの更新操作を指示する保守用管理サーバにより構成されるコンピュータシステムにおいて、前記制御プログラム内蔵型装置と前記保守用管理サーバは、公衆回線網で接続され、前記制御プログラム内蔵型装置と前記制御プログラム配信装置は、インターネットで接続され、前記保守用管理サーバから、前記制御プログラム内蔵型装置に対して制御プログラムの更新指示を行う場合、まず、前記保守用管理サーバから前記制御プログラム内蔵型装置に、前記制御プログラム配信装置との接続に必要な認証情報を公衆回線網を経由して送信し、次に前記制御プログラム内蔵型装置が、前記認証情報をインターネット経由で前記制御プログラム配信装置へ送信し、前記制御プログラム配信装置との接続を確立した後、前記制御プログラム内蔵型装置が、前記制御プログラム配信装置から該制御プログラムの転送を行い、該制御プログラムの転送終了後、前記制御プログラム内蔵型装置の制御プログラムの更新処理を実行することを特徴とする制御プログラム内蔵型装置のプログラム更新方式。

【請求項 2】

請求項 1 に記載の制御プログラム内蔵型装置のプログラム更新方式において前記保守用管理サーバから前記制御プログラム更新指示および前記認証情報を受信する保守通信手段と、前記制御プログラム配信装置から転送される制御プログラムを受信するデータ通信手段と、前記データ通信手段により受信した制御プログラムを、該制御プログラム制御装置の制御プログラム格納領域に格納するプログラム更新手段とを備えることを特徴とする制御プログラム内蔵型装置。

【請求項 3】

請求項 1 に記載の制御プログラム内蔵型装置のプログラム更新方式において、

更に、一方をローカルエリアネットワークにより前記制御プログラム内蔵型装置と接続し、もう一方をインターネットと接続した中継装置を備え、前記制御プログラム内蔵型装置が前記中継装置に、前記制御プログラム配信装置からの制御プログラム転送を指示し、該指示に基づき、前記中継装置は、前記制御プログラム配信装置からの該制御プログラムの転送を実行する、または、既に該制御プログラムが前記中継装置に転送済みである場合は、転送は実行しないことを特徴とする制御プログラム内蔵型装置のプログラム更新方式。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、コンピュータシステムに適用される制御プログラム内蔵型装置に係わり、遠隔地からの指示で制御プログラムの配信および更新を自動的にかつ安全に実施する技術に関し、特に制御プログラムの配信にインターネットを使用するのに好適なプログラム自動更新方式に関する。

【0002】

【従来の技術】

コンピュータシステムを構成する多くの装置は、その装置の機能を実現する為の制御プログラムが内蔵されている。この制御プログラムは、装置ベンダーが、装置ハードウェアの設計と一体となって開発することが一般的である。このような制御プログラムを内蔵型装置も、他のソフトウェアと同様、新たな機能追加、性能向上または動作不具合対策などの理由で、制御プログラムの更新が必要であることは周知の事実である。このような制御プログラムの更新は、従来、図7で示すようなシステムで行われるのが一般的である。

【0003】

図7において、保守センター701は各地に点在するコンピュータセンターの稼動状態の監視、障害発生時の原因究明および障害対策をなどの保守作業を指示する拠点であり、これら保守作業指示を行うための保守用管理サーバ702を備えている。保守センター701と保守対象であるコンピュータセンター707とは公衆回線網103で接続されている。開発センター705は、コンピュータセ

ンター 7 0 7 に設置されている制御プログラム内蔵型装置 7 1 0、7 1 1、7 1 2 の制御プログラムの開発を行う拠点であり、開発された制御プログラムが格納されている制御プログラム配信サーバ 7 0 6 が設置されている。制御プログラム配信サーバ 7 0 6 には装置の種類に対応した最新の制御プログラムや、一時的な障害対策のための部分的なプログラム（パッチ）が格納されている。制御プログラム配信サーバ 7 0 6 は専用回線 7 0 4 を使用して保守センター 7 0 1 と接続され、制御プログラム更新情報および制御プログラムのファイル配信が可能となっている。コンピュータセンター 7 0 7 は、保守対象である制御プログラム内蔵型装置 7 1 0、7 1 1、7 1 2 と、それら装置の操作を行うためのコンソール装置 7 0 8 などから構成されている。制御プログラム内蔵型装置 7 1 0 は公衆回線網 1 0 3 に接続されていて、保守センター 7 0 1 との通信を制御する。また、各制御プログラム内蔵型装置間はローカルエリアネットワーク（LAN）7 0 9 で接続されていて、保守センター 7 0 1 からの制御プログラム内蔵型装置 7 1 1、7 1 2 への保守操作を制御プログラム内蔵型装置 7 1 0 経由で実行できるようになっている。制御プログラムの更新が必要となった場合、まず、保守センター 7 0 1 から保守用管理サーバ 7 0 2 を使用して、開発センター 7 0 5 に設置されている制御プログラム配信サーバ 7 0 6 から必要な制御プログラムを専用回線 7 0 4 を経由して、保守センター 7 0 1 へ転送する。

【0 0 0 4】

次に、保守センター 7 0 1 から、制御プログラム更新作業が必要となったコンピュータセンター 7 0 7 の制御プログラム内蔵型装置 7 1 0 に対して公衆回線網 7 0 3 を使用して接続を行い、更新された制御プログラムの転送および制御プログラム更新処理の実行を指示する。指示を受けた、制御プログラム内蔵型装置は、内部にて制御プログラム更新処理を実行する。

【0 0 0 5】

【発明が解決しようとする課題】

上記従来技術は、制御プログラムを配信するために保守センターと開発センターの間に専用回線を設置する必要がある。専用回線を設置すれば、回線提供者への継続的な回線使用料金の支払いが発生する。また、仮に専用回線でなく公衆

回線を使用したとしても、制御プログラムを転送する毎に、回線使用料が発生することとなる。近年の制御プログラム内蔵型装置の機能向上に伴い、制御プログラムの規模も大きくなっているため、公衆回線のように低速かつ、距離、使用時間に応じて課金される仕組みでは、今後ますます、回線使用料が上がる一方である。

【 0 0 0 6 】

一方、上記従来技術は、保守センターとコンピュータセンター間の制御プログラム転送にも公衆回線網を使用している。複数のコンピュータセンターへ制御プログラムを転送する場合、コンピュータセンター毎に転送を繰り返さなくてはならないため、対象となるコンピュータセンターの数に比例して、転送に要する時間と回線使用料負担が増加することとなる。

【 0 0 0 7 】

本発明の目的は、このような従来の問題を解決し、制御プログラムを各コンピュータセンターへ転送する時間を短縮し、かつ回線使用料金を削減し、制御プログラム更新に要する時間およびコストの低減を可能とする制御プログラム内蔵型装置のプログラム更新方式を提供することである。

【 0 0 0 8 】

【課題を解決するための手段】

上記目的を達成するため、本発明は、制御プログラム内蔵型装置に、保守センターの保守用管理サーバから制御プログラム更新指示および制御プログラム配信サーバとの接続に必要な認証情報を受信する保守通信手段と、制御プログラム配信サーバから転送される制御プログラムを受信するデータ通信手段と、データ通信手段により受信した制御プログラムを、制御プログラム制御装置内の制御プログラム格納領域に格納するプログラム更新手段とを備える。制御プログラム内蔵装置の保守通信手段と保守用管理サーバは、従来と同様、公衆回線網で接続する。

【 0 0 0 9 】

さらに、一方をローカルエリアネットワークにより制御プログラム内蔵型装置と接続し、もう一方をインターネットと接続した中継装置を備える。

【0010】

保守用管理サーバから、制御プログラム内蔵型装置に対して制御プログラムの更新指示を行う場合は、まず保守用管理サーバから前記制御プログラム内蔵型装置に、制御プログラム配信サーバとの接続に必要な認証情報を公衆回線網を經由して送信し、次に、制御プログラム内蔵型装置が、認証情報を中継装置経由とインターネットを經由して、制御プログラム配信サーバへ送信し、制御プログラム配信サーバとの接続を確立した後、中継装置が、制御プログラム配信サーバから制御プログラムの受信を行う。制御プログラムの受信終了後、さらに制御プログラム内蔵型装置に制御プログラムの転送を行い、転送終了後、制御プログラム内蔵型装置の制御プログラムの更新処理を実行を行う。また、既に制御プログラムが中継装置に転送済みである場合は、制御プログラム配信サーバからの制御プログラム転送は実行はしないで、転送済みの制御プログラムを制御プログラム内蔵型装置に転送する。

【0011】

以上のように、既に設置されているインターネットを使用することで、制御プログラム転送に要する時間が削減でき、また複数コンピュータセンター同時転送も可能となる。また、制御プログラム更新指示、認証情報は保守センターから公衆回線経由で直接コンピュータセンターへ送信することで、第三者による故意の制御プログラム更新を防ぐことができる。

【0012】

【発明の実施の形態】

以下、図を用いて、本発明の一実施形態について説明する。

【0013】

図1は、本発明のプログラム自動更新方式を適用したシステムの一実施形態の構成を示すブロック図である。保守センター101は各地に点在するコンピュータセンターの稼動状態の監視、障害発生時の原因究明および障害対策をなどの保守作業を指示する拠点であり、これら保守作業指示を行うための保守用管理サーバ102を備えている。保守センター101と保守対象であるコンピュータセンター107とは公衆回線網103で接続されている。コンピュータセンター10

7で障害が発生すると、公衆回線網103を経由してコンピュータセンター107から障害発生メッセージが保守センター101に報告される。また、保守センター101から保守作業が必要となった場合には、保守センター101から、コンピュータセンター107に対して公衆回線網103を使用して回線接続を行い必要な保守作業を実施する。

【0014】

コンピュータセンター107は、例えば、保守対象であるディスク制御装置DKC110、DKC111、およびDKC112と、それら装置の操作を行うためのリモートコンソール(RMC)108から構成されている。DKC110は公衆回線網103に接続されていて保守センター101との通信を制御する。

また、各DKC間はローカルエリアネットワーク(LAN)で構成されるDKC保守用LAN109で接続されていて、保守センター101からのDKC111、112への保守操作をDKC110経由で実行できるようになっている。RMC108も同様にLAN109を経由してコンピュータセンター内に設置されているすべてのDKC110、111、112の操作が実行できるようになっている。

【0015】

本実施形態の説明では保守対象となる制御装置は3台であるが、本発明を適用したシステムにおいては台数は何台あっても構わない。また、保守対象に中央処理装置(CPU)などの他の種類の装置が含まれていても構わない。

【0016】

図1の各々のDKC110、111、112は、上位HOST113と接続されていることを示している。

【0017】

開発センター105は、コンピュータセンター107に設置されているディスク制御装置DKC110、111、112の制御プログラムの開発を行うセンターであり、開発された制御プログラムが格納されている制御プログラム配信サーバ106が設置されている。制御プログラム配信サーバ106には制御装置の種類に対応した最新の制御プログラムや、一時的な障害対策のための部分的なプロ

グラム（パッチ）が格納されている。制御プログラム配信サーバ106はインターネット104へ接続されていて、保守センター101、コンピュータセンター107への情報提供、ファイル転送が可能となっている。

【0018】

コンピュータセンター107に設置されているディスク制御装置DKC110、111、112に内蔵されている制御プログラムの更新は次の手順で実行される。まず、保守センター101に設置されている保守用管理サーバ102から制御プログラムの配信と更新の指示が公衆回線網103を経由してDKC110に行われる。指示を受け取ったDKC110はRMC108に対して制御プログラム配信サーバ106からの制御プログラムダウンロードの指示を行う。次に、RMC108はインターネット104を経由して制御プログラム配信サーバ106から制御プログラムのダウンロードを実施する。そして、ダウンロードされた制御プログラムは一旦RMC108内に格納された後、DKC110、111、112へ転送される。DKC110、111、112に転送された制御プログラムの更新は、各DKC内部で実行される。

【0019】

図2は、コンピュータセンター107に設置されるDKC110の内部に具備されているSVP910が制御プログラム更新方式を実施する際のソフトウェア構成を示すブロック図である。SVP910は、公衆回線網103と接続して保守センター101との通信を制御する保守センター通信部201、他DKC111、112、RMC108とのDKC保守用LAN109経由の通信および開発センター105に設置されている制御プログラム配信サーバ106からの制御プログラムのダウンロードを制御するDKCダウンロード制御部205、ダウンロードした制御プログラムを格納するプログラム格納部206、プログラム格納部206に格納された制御プログラムを内蔵されているプロセッサのメモリーに展開するプログラム更新制御部202、そしてプログラム更新対象となるCHA、DKA内プロセッサと通信するためのDKC内部LAN813とから構成されている。プログラム自動更新処理の動作に関しては、後で図4から6を用いて詳しく説明する。

【0020】

図3は、コンピュータセンター107に設置されるRMC108の制御プログラム更新方式に関連する構成を示すブロック図である。RMC108は、インターネット104およびDKC保守用LAN109と接続するRMCダウンロード制御部301、DKCの制御プログラムを一時的に格納するプログラム格納部302とから構成されている。

【0021】

次に、図4から図6を用いて制御プログラム自動更新処理の動作に関して詳しく説明する。

【0022】

図4は、保守センター101から制御プログラムの自動配信と自動更新の連続実行指示を行った場合の処理動作を示すシーケンス図である。まず、保守用管理サーバ102からDKC110の保守センター通信部201に対して制御プログラム種別 (Program Type)、プログラムバージョン (Program Version)、対象となるDKCのシリアル番号 (S/N) および認証情報等を公衆回線網で送付する (処理101-S1)。保守センター通信部201は処理201-S2で受信した前記情報をDKCダウンロード制御部205に送付して制御プログラムのダウンロード開始を指示する (処理201-S2)。指示を受けたDKCダウンロード制御部205は、LAN109を経由して処理205-S1で受信した制御プログラム種別、プログラムバージョン、シリアル番号、認証情報をRMC108で動作するRMCダウンロード制御部301に送付して、開発センター105にある制御プログラム配信サーバ106からの制御プログラムダウンロードの実行を指示する (処理205-S2)。RMCダウンロード制御部301は、処理301-S1で受信した情報に該当するプログラムがプログラム格納部302に格納されているかどうか調べ、その結果をDKCダウンロード制御部205に応答する。以降、プログラム格納部302にはプログラムが格納されていないことを前提に説明を進める。

【0023】

したがって、今段階では、インターネット制御部301はDKCダウンロード

制御部 2 0 5 に対してファイル未取得の状態を応答する（処理 3 0 1 - S 2）こととなる。これにより、インターネット制御部 3 0 1 は制御プログラム配信サーバ 1 0 6 からの該当制御プログラムのダウンロード処理を開始する。ダウンロードを行う場合、まず最初に、RMC ダウンロード制御部 3 0 1 は保守用管理サーバ 1 0 2 から発信された認証情報を制御プログラム配信サーバ 1 0 6 に送信する（処理 3 0 1 - S 3）。認証情報を受信した（処理 1 0 6 - S 1）制御プログラム配信サーバ 1 0 6 は、認証情報の照合を行い、その結果をインターネット制御部 3 0 1 に応答する。ここでは照合結果に問題がないものとし、OK を応答する（処理 1 0 6 - S 2）。認証に問題ないことを受信したインターネット制御部 3 0 1（処理 3 0 1 - S 4）は、次に、制御プログラムを構成するファイル情報の送信を制御プログラム配信サーバ 1 0 6 に要求する（処理 3 0 1 - S 5）。要求を受信した制御プログラム配信サーバ 1 0 6 は、ファイル情報を RMC ダウンロード制御部 3 0 1 に送信する（処理 1 0 6 - S 3、S 4）。RMC ダウンロード制御部 3 0 1 は受け取ったファイル情報（処理 3 0 1 - S 6）により、制御プログラム配信サーバ 1 0 6 にファイル転送要求を行い（処理 3 0 1 - S 8）、要求を受けた制御プログラム配信サーバ 1 0 6 は、該当するファイルを RMC ダウンロード制御部 3 0 1 に送信する（処理 1 0 6 - S 5、S 6）。

【 0 0 2 4 】

RMC ダウンロード制御部 3 0 1 は、受信したファイルをプログラム格納部 3 0 2 に順次格納し（処理 3 0 1 - S 1 0）、要求したすべてのファイルを格納し終えたら、ファイル内容整合性を検査を実施する（処理 3 0 1 - S 1 1）。

【 0 0 2 5 】

一方、先にファイル未取得状態の応答を受信した（処理 2 0 5 - S 3）DKC ダウンロード制御部 2 0 5 は、定期的な間隔で、RMC ダウンロード制御部 3 0 1 に対してファイル取得状態入手コマンドを発行する。ファイル取得が終了していない間のファイル取得状態入手コマンド（処理 2 0 5 - S 4）に対しては、RMC ダウンロード制御部 3 0 1 はファイル取得中の状態を応答する（処理 3 0 1 - S 9）。

【0026】

ファイル取得中状態を受信したDKCダウンロード制御部205（処理205-S5）は、一定時間経過後、再度ファイル取得状態入手コマンドを発行し状態を入手する（処理205-S5、301-S12、301-S13、205-S7）。ファイル取得状態がファイル取得完了であれば、次に、制御プログラム転送手続き開始要求をRMCダウンロード制御部301に行う（処理205-S8）。

【0027】

要求を受け取った（処理301-S14）RMCダウンロード制御部301は、要求許可を応答し（処理301-S15）、許可を受信したDKCダウンロード制御部205は、RMCダウンロード制御部301が制御プログラムサーバ106からファイルをダウンロードする場合の手続きと同様に、制御プログラムを構成するファイル情報入手要求をRMCダウンロード制御部301に行って（処理205-S10）、ファイル情報を入手（処理301-S16、処理301-S17、処理205-S11）して、その後、ファイル転送をRMCダウンロード制御部301に要求する（処理205-S12）。

【0028】

RMCダウンロード制御部301は、ファイルをRMC108内のプログラム格納部302から読み出し、DKCダウンロード制御部205に送信する（処理301-S18、301-S19）。DKCダウンロード制御部205は、受信したファイルをプログラム格納部206に順次格納し（処理205-S13）、要求したすべてのファイルを格納し終えたら、ファイル内容整合性の検査を実施する（処理205-S14）。

【0029】

ファイル内容整合性検査終了後、DKCダウンロード制御部205は、ファイル転用要求終結をRMCダウンロード制御部301に送信する（処理205-S15）。終結通知を受信した（処理301-S20）RMCダウンロード制御部301は、確認応答をDKCダウンロード制御部205に送信（処理301-S21）し、その確認要求をDKCダウンロード制御部205が受け取ることで（

処理 2 0 5 - S 1 6) すべての制御プログラムダウンロード処理が終了する。

【 0 0 3 0 】

ダウンロード処理が終了したらDKCダウンロード制御部 2 0 5 は、自動配信が終了したところを通知するサービス情報メッセージ (S I M) を保守センター保守用管理サーバ 1 0 2 に報告する (処理 2 0 5 - S 1 7、処理 1 0 2 - S 2)。

【 0 0 3 1 】

次に、DKCダウンロード制御部 2 0 5 は、ダウンロードした制御プログラムを適用するために、プログラム交換をプログラム更新制御部 2 0 2 に指示する (処理 2 0 5 - S 1 8)。指示を受けたプログラム更新制御部 2 0 2 は (処理 2 0 2 - S 1)、プログラム格納部 2 0 6 から該当制御プログラムを読み出し、C H A、D K A に具備するプロセッサの制御プログラムの交換処理を実行する (処理 2 0 2 - S 2)。プログラム交換処理が終了すると、プログラム更新制御部 2 0 2 は、自動更新が終了したところを通知するサービス情報メッセージ (S I M) を保守用管理サーバ 1 0 2 に報告する (処理 2 0 2 - 3、処理 1 0 2 - S 3)。

【 0 0 3 2 】

以上でプログラム自動更新処理が終了し、保守用管理サーバ 1 0 2 から指示を受けた制御プログラムの自動配信・自動更新の連続実行処理が終了する。

【 0 0 3 3 】

図 5 は、自動配信のみを実行する場合の動作を示したシーケンス図である。基本的には図 4 の自動配信・自動更新の連続実行動作の自動配信動作と同じであり、DKC内部のプログラム格納部 2 0 6 に制御プログラムを格納した時点で処理を終了する。

【 0 0 3 4 】

図 6 は、自動更新のみを実行する場合の動作を示したシーケンス図である。図 5 の自動配信のみ終了した状態から、実際に制御プログラムの更新を適用する場合に使用することができる。まず、図 4 シーケンスと同様に、保守用管理サーバ 1 0 2 からDKC 1 1 0 の保守センター通信部 2 0 1 に対して制御プログラム種別 (Program Type)、プログラムバージョン (Program Version)、対象となるDKCのシリアル番号 (S/N) および認証情報を公衆回線網で送付する (処理 1

01-S1)。保守センター通信部201は処理201-S1で受信した前記情報をDKCダウンロード制御部205に送付する(処理201-S2)。指示を受けたDKCダウンロード制御部205は、プログラム更新制御部202に対して該当制御プログラムの交換指示(処理205-S2)を行う。指示を受けたプログラム更新制御部202は(処理202-S1)、図4シーケンスと同様に該当制御プログラムの交換処理を実行する(処理202-S2)。

【0035】

制御プログラム交換処理が終了すると、プログラム更新制御部202は、自動更新が終了したところを通知するサービス情報メッセージ(SIM)を保守用管理サーバ102に報告して(処理202-3、処理102-S2)、制御プログラムの自動更新処理が終了する。

【0036】

図8は、DKC110の内部構造を示したハードウェア構成図である。DKC110は、HOST113との接続I/Fを制御する複数のチャネルアダプタ(CHA)801、HDD821とのI/Fを制御する複数のディスクアダプタ(DKA)802、これらアダプタ間のデータ転送を実施するためのSwitch810、HOST113から転送されたデータを一時保持するCache811、本DKC110の構成情報を保持し全アダプタが共通に使用することの出来る共有メモリ812、DKC110の障害監視、障害発生時のリカバリ指示、または本発明で述べる制御プログラムの交換指示を実施するSVP910、及び当該SVPと各アダプタ間との保守情報を通信するためのDKC内部LAN813から構成される。SVP910は、さらにDKC保守用LAN109と接続することで、他のDKC111、112との保守データの送受を行う。本発明での制御プログラムとは、各アダプタに搭載されているプロセッサで動作するプログラムのことで、SVPから制御プログラムを転送し、SVPからの指示で各アダプタのプロセッサが閉塞、交換、回復を実施する。制御プログラムの交換は、DKC110がHOST113とのI/Oを受け付け、処理を実施している最中でも可能となっている。

【0037】

図9はSVP910の内部構造を示したハードウェア構成図である。SVPは、パーソナルコンピュータであって、パーソナルコンピュータが一般に具備する各種ハード部品から構成されている。SVP910は、DKC保守用LAN109とのLAN I/F、DKC内部LAN813とのLAN I/F、及び公衆回線網103と接続するためのModemを具備しているところが特徴である。

【0038】

図10は、RMC108の内部構造を示したハードウェア構成図である。RMCは、SVPと同様、パーソナルコンピュータであって、パーソナルコンピュータが一般に具備する各種ハード部品が構成されている。RMC108は、インターネット104とのLAN I/F、DKC保守用LAN109とのLAN I/Fを具備しているところが特徴である。

【0039】

図11は、本実施例で示す各センタ間のデータの流れを示したデータフロー図である。以下に、本実施例で示すデータの流れを順を追って説明する。

【0040】

保守管理サーバ102は、交換対象とするDKCの装置タイプ、製造番号（以下S/Nと呼ぶ）、交換する制御プログラムのバージョン、及び更新モードのデータ入力を受け付ける。これらの入力データは、図中では1011で示している。図13は、データ1011のデータフォーマット、及び具体的な値を例として示している。また先の説明では、制御プログラム種別（Program Type）を用いているが、ここでは装置タイプ、装置型式として説明する。両データを対象としてもよい。図12では、保守管理サーバ102上で表示する更新指示画面の例を示している。ここで、更新モードとしては次の3種類から選択できるようになっている。

【0041】

“Download&Update”モードは、制御プログラムをDKCへダウンロードし、制御プログラムの交換を実施するモードである。“Download”モードは、制御プログラムをDKCへダウンロードするが、制御プログラ

ムの交換は指示しないモードである。これは、顧客のコンピュータセンター107運用計画上、交換時期を別の機会に実施する必要が生じた場合に選択する。これにより、交換可能な時期となった場合に、“Update”モードを選択することで交換処理が実行される。“Update”モードは、あらかじめ“Download”モードで転送されている制御プログラムを用いて、交換処理のみ実施するモードである。

【0042】

図12では、3台のDKCに対して、各々“Download&Update”モード、“Download”モード、及び“Update”モードを指示しているところを示している。また、適用バージョンは、“01-02-35-67/00”、装置タイプは“H-65A1-1”を入力している。これらの入力したデータは、図13で示す1011のデータフォーマットとして保守用管理サーバ102で入力される。他のDKCについても、1011のデータフォーマットで示される。

【0043】

図11で示す通り、データ1011で入力を受け付けた保守用管理サーバ102は、データ1012としてDKC110へ公衆回線網103を用いて転送する。データ1012のデータフォーマットは図14で示す。図14は、保守用管理サーバ102がSVP910に対して転送するデータ1012のデータフォーマットを示す。図14でもわかる通り、データ1011のデータフォーマットに、SVP認証キー（SVPへ接続するためのログインとパスワード）、開発センタ105内の制御プログラム配信サーバ106へ接続するのに必要な配信サーバ認証キー（ログインとパスワード）、及び制御プログラム配信サーバ内にある制御プログラムのファイルロケーションを追加している。SVP認証キーは、図14では1つのデータフォーマット内で示しているが、実際には、公衆回線網103を用いてDKC110内のSVPと接続するのに、最初にデータ転送されるべきものである。このSVP認証キーは、公衆回線網といえども不正に接続されないようセキュリティ上必要である。ここではSVP認証キーを固定値として扱っている。これは、保守用管理サーバ102とSVP910との間のプロトコルでロ

グイン・パスワードの更新ロジックを実現すれば可変となることは明白である。また、配信サーバ認証キーは、本実施例では固定値として扱う。RMC 1 0 8 が制御プログラム配信サーバ 1 0 6 と接続する際に必要となる情報である。ファイルロケーションは、装置型式と制御プログラムバージョンから一意的に決定することのできる情報である。あらかじめ制御プログラム配信サーバ 1 0 6 上に保持する制御プログラムの配置方法にルールを持たせた方法で実現している。

【 0 0 4 4 】

図 1 1 で示す通り、1 0 1 2 データフォーマットで受け取った DKC 1 1 0 の SVP 9 1 0 は、RMC 1 0 8 に対して 1 0 1 3 データフォーマットでデータを送信する。1 0 1 3 データフォーマットは、図 1 5 で示す。図 1 5 は、DKC 1 1 0 の SVP 9 1 0 から RMC 1 0 8 に対して送信する 1 0 1 3 のデータフォーマットを示した図である。図 1 5 で示す通り、1 0 1 2 データフォーマットから、SVP 認証キーを削除したデータフォーマットが 1 0 1 3 である。

【 0 0 4 5 】

図 1 1 において、1 0 1 3 データフォーマットを受け取った RMC 1 0 8 は、インターネット 1 0 4 を用いて制御プログラム配信サーバ 1 0 6 と接続する。このとき、データフォーマット 1 0 1 3 でアクセスする。具体的な実現例としては、TCP/IP のファイル転送プロトコルである f t p を用いる。制御プログラム配信サーバ 1 0 6 との接続では、配信サーバ認証キーを用いる。接続に成功すると、制御プログラム配信サーバ 1 0 6 から制御プログラム 1 0 1 5 を返信する。RMC 1 0 8 は、受け取った制御プログラム 1 0 1 5 を各 DKC へ転送・交換指示を行う。この時、既に SVP 9 1 0 より受信したデータ 1 0 1 3 で示される更新モードに基づいて指示することも可能である。SVP 9 1 0 では、制御プログラム 1 0 1 5 を受け取り、各アダプタに実装するプロセッサに対して制御プログラム交換を指示し、交換処理の結果を受け取る。その後、SVP 9 1 0 は、交換処理結果 1 0 1 7 を公衆回線網 1 0 3 を用いて保守用管理サーバ 1 0 2 へ転送する。

【 0 0 4 6 】

図 1 6 は、交換処理結果 1 0 1 7 を受け取った保守用管理サーバ 1 0 2 が表示

する更新結果一覧画面を示した図である。製造番号 3 0 0 5 1、3 0 0 5 3 で示した D K C は指示通りの交換処理を実施したことを示す。また 3 0 0 5 2 で示した D K C は交換処理に失敗し、異常終了していることを示す。図 1 6 で示す“(7 9 F 4) ”は異常終了の詳細を示すエラーコードで、これにより、次のリカバリ対策が迅速に実施できるように示している。

【 0 0 4 7 】

また図 1 7 は、保守用管理サーバ 1 0 2 から、現在の D K C の更新状態を取得した結果を表示した例である。D K C 内の S V P と保守管理サーバとのプロトコルにおいて、このような D K C の制御プログラム更新状態を取得する I / F を具備すれば、現行稼働中の Version、配信 (U p l o a d) されている Version 等を表示することが出来る。これにより、次の制御プログラム更新指示を保守用管理サーバ 1 0 2 から指示することが可能となる。

【 0 0 4 8 】

本実施例では、配信サーバ認証キー及び制御プログラムのファイルロケーションを固定値として扱う方法について述べた。

【 0 0 4 9 】

次に、配信サーバ認証キーと制御プログラムのファイルロケーションを、更新要求が発生するたびに取得する方法について述べる。

【 0 0 5 0 】

図 1 8 は、第 2 の実施例を実施するデータフロー図である。図 1 8 は、図 1 1 で示した制御プログラム配信サーバ認証キー、及び制御プログラムのファイルロケーションを、保守用管理サーバ 1 0 2 が 1 0 1 1 データの入力を受け付けた後に制御プログラム配信サーバ 1 0 6 から取得する流れを加えたものである。保守用管理サーバ 1 0 2 と制御プログラム配信サーバ 1 0 6 とは、インターネット 1 0 4 で接続されている。保守用管理サーバ 1 0 2 は、入力データ 1 0 1 1 を用いて制御プログラム配信サーバ 1 0 6 と接続し、データフォーマット 1 0 1 3 を取得する。この後の制御は、前実施例で述べた通りである。これにより、固定値として扱っていた認証キーとファイルロケーションを適宜取得することが可能となり、保守センタ 1 0 1 及び開発センタ 1 0 5 の運用を各々独立化することが可能

となる。これらの2つのセンタは通常同一会社が運用するのが基本であるが、昨今保守センタのみを提供する保守会社が存在し、必ずしも同一でない場合が多い。このような場合、相互の取り決めをあらかじめ決定し運用する必要が無くなる。

【0051】

さらに、第2の実施例では、認証キーを各要求のあったDKC毎に発行することとなるので、RMC108からの取得要求に対して、発行済み認証キーとの一致チェックが可能となる。具体的には、保守用管理サーバ102で受け付けた交換要求に対して、開発センタ105から認証キーを発行する（これは、データ1013内に含まれている）。開発センタ105は、発行済みの認証キーを保持しておき、RMC108からの接続要求時に送信されてくる認証キーと照合する。送信された認証キーが、既に発行済みの認証キーであるかどうか、また適用するDKCの装置タイプ、製造番号と一致しているか等をチェックする。チェックの結果、一致していれば、RMC108からの要求が正しいものと判断し、該当する制御プログラム1015を返信する。この認証ロジックを実施するための開発センタ105側の制御プログラム配信サーバ106で具備すべきソフトウェア構成を図19で示す。

【0052】

図19は、制御プログラム配信サーバ106で実施するソフトウェア構成図である。認証キー発行受付1901は、保守用管理サーバ102より発信されたデータ1011を受け付ける。認証キー生成1902は、受け付けたデータ1011に基づいて認証キーを生成し、発行済認証キー1904へ格納する。認証キー発行1903は、生成した認証キー、及び制御プログラムのファイルロケーション情報を付加して、保守用管理サーバ102へデータ1013として送信する。さらに、制御プログラム配信受付1911は、RMC108より送信された配信要求であるデータ1013を受け付ける。発行認証キーチェック1912は、データ1013に含まれる認証キーが、発行済認証キー1904で保持されている既に発行済の認証キーと一致しているかどうかを判断する。一致していた場合は、制御プログラム転送1913より制御プログラム1015をRMC108へ送

信する。一致していない場合は、RMC108からのアクセスを拒否する。

【0053】

以上の実施例では、保守用管理サーバ102で入力した更新情報に基づいて、制御プログラムの交換を実施する例について説明した。更に、インターネット104を利用して、DKC110, 111, 112を保持する顧客自身が、更新要求を発行する場合を想定する。以下に、顧客自身が更新要求を発行する場合の第3の実施例について述べる。

【0054】

第3の実施例では、顧客自身が更新要求を発行する方法について述べる。元来、顧客はDKC110, 111, 112を販売会社から購入する。通常、装置製造会社と販売会社とは一致しているが、昨今、OEM販売等にも見られる通り、製造会社と販売会社が異なる場合がある。このとき、装置製造会社が制御プログラムを改良し、その改良点を販売会社へ伝達する。この販売会社が、制御プログラムの改良点を顧客に提示し、顧客からのバージョンアップ要求を受け付け、プログラム改良版をリリースする販売形態は、既に通常の販売業務として実施されている。

【0055】

本実施例では、顧客がこうしたバージョンアップ情報に基づいて、当該DKCのプログラム更新を欲した場合を想定する。

【0056】

図20は、顧客が更新要求を発行する場合のデータフローを示した図である。第2の実施例でしめしたデータフロー図（図18）との相違点は、顧客オフィス2010と顧客管理センタ2001とを具備した点である。

【0057】

顧客は、顧客オフィス2010にある要求入力2011から更新要求を発行する。顧客は、コンピュータセンタ107を運用・管理している。図20で示す通り、必ずしも運用・管理責任者である顧客は、コンピュータセンタ107に常駐しているとは限らない。したがって、コンピュータセンタ107とは別の顧客オフィス2010に常駐していることを想定する。

【0058】

また、顧客管理センタ2001は、DKC装置の販売会社であることを想定している。この顧客管理センタ2001では、顧客に関する情報を管理している。また開発センタ105は、DKC装置の製造会社であることを想定している。

【0059】

顧客は、要求入力2011を用いてデータ2003を入力する。2003の詳細は、図22で示す。図22は、データ2003のデータフォーマット図である。図22で示す通り、データ2003は、データ1011に“顧客情報”を具備したフォーマットで構成する。図22で示す“顧客情報”は、会社名を値としている。この情報は、会社名だけでなく会社の担当責任者名、部署名、また、顧客の会社と販売会社との間で取り交わしている取引口座に関する情報でもよい。

【0060】

これらの情報をインターネット104を用いて顧客管理センタ2001に設置されている顧客情報管理サーバ2002へ伝達する。この通信路は、取引に関わる情報を有しているので、あらかじめ暗号化する必要がある。通信路の暗号化は、SSLやVPNなどの技術が一般に知られている。

【0061】

また、顧客情報管理サーバ2002は、受信した2003データを1011データに変換して保守管理サーバ102へ転送する。実質、2003データから顧客情報を削除することで1011データを生成することができる。1011データを受信した後の動作は、第2の実施例で示した通りである。最後に、交換処理が完了し各DKCより受信した交換処理結果1017を顧客情報管理サーバ2002へ転送するとともに、顧客情報管理サーバ2002は、さらに顧客の要求入力2011へ転送する。転送手段は、メールであってもかまわない。これは、顧客が要求を入力してから、交換結果1017を受信するまでの時間が長い分、実用的であると考ええる。

【0062】

以上の実施例では、保守センタ101とコンピュータセンタ107との間を公衆回線網103で接続した形態について説明した。この間の実装方法をLANで

用いた場合のハードウェア接続構成について説明する。図21は、保守センタ101とコンピュータセンタ107との間を、公衆回線網103でTCP/IPのネットワークとして接続したときのハードウェア接続構成図である。

【0063】

この場合、保守センタ101とコンピュータセンタ107との間に各々ダイヤルアップルータ2101、2102を接続する。これにより、DKC装置の保守情報をTCP/IPによるコンピュータネットワークとして実現することが可能となる。これは、本発明で説明している制御プログラムの転送だけでなく、DKC装置の保守情報（障害情報等）の伝達手段にも応用することが可能となる。

【0064】

図23は、要求入力2011のソフトウェア構成図である。最新Version取得2301は、顧客から装置型式（タイプ）とその製造番号（S/N）の入力を受け付け、顧客情報管理サーバ2002へ伝達する。顧客情報管理サーバ2002での動作は、図24を用いて後で説明する。顧客情報管理サーバ2002は、保守管理サーバ102を経由して、DKC110、111、112から最新Version情報を入手し、要求入力2011へ返信する。最新Version取得2301は、取得したVersionをCRT等へ結果出力するとともに、Version情報2302へ格納する。取得に時間がかかる場合は、その旨のメッセージを表示して、顧客とのI/Fを一旦終了することも可能である。この場合、顧客情報管理サーバ2002から受け取ったVersionを一旦Version情報2302に格納し、別の契機で顧客が格納しているVersion情報を参照することも可能である。

【0065】

更新要求2303は、顧客からの更新要求を受け付ける。この場合、装置型式・製造番号・更新したいバージョン及び顧客情報を入力する。入力の際、Version情報2302に格納されている情報を用いることで利便性を図ることが可能である。入力後、更新要求2303は、データ2003を顧客情報管理サーバ2002へ転送する。更新結果は1017として顧客情報管理サーバ2002より受信し、出力する。この場合も、処理に時間がかかることがあるので、一旦

メッセージを表示し、顧客とのI/Fを終了した後、更新結果を受信、格納し、別の機会に顧客へ出力することも可能である。

【0066】

図24は、顧客情報管理サーバ2002のソフトウェア構成図である。

【0067】

Version取得制御2401は、要求入力2011より送信された、顧客からの最新Version取得要求を保守用管理サーバ102へ転送し、保守用管理サーバ102が取得した最新Version情報をサーバ102より受信、結果を要求入力2011へ返信する制御を実施する。更新受付2402は、要求入力2011より送信された2003データを受信する。これは顧客の要求した更新情報である。更新指示2404は、2003データに基づいてどの顧客が要望したのかを顧客DB2403より検索し、更新指示をデータ1011として保守用管理サーバ102へ転送する。また更新指示した内容を顧客情報とともに更新状態DB2405へ格納する。交換完了受付2405は、保守用管理サーバ102より更新結果1017を受信し、当該結果がどの顧客から要求されたものなのかを更新状態DB2405より検索し、顧客情報に基づいて結果を顧客結果報告処理で要求入力2011へ返信する。課金処理2406は、更新結果が正常終了を示していた場合、当該顧客に対して課金を実施する。具体的には、あらかじめ契約されている取引口座に対して引き落としの指示を実施する。または、あらかじめ登録されている顧客のクレジットカードNo.に基づいて、カード会社への支払指示を実施するものである。この実現方法はインターネット104を用いることで、自動化可能である。

【0068】

上述の実施例では、保守センタ101とコンピュータセンタ107とを公衆回線網103経由で接続していたのを、すべてインターネット104で実施する方法も可能である。この場合、保守センタ101とコンピュータセンタ107の各DKC110, 111, 112とは、セキュリティの確保が必要となる。この場合、Virtual Private Network (VPN) といった、セキュリティを確保されたTCP/IP接続形態や、SSLといった暗号された通信

レイヤを使用することで可能となる。また、上述の実施例で示したように、SVPに対する認証キー情報を有しているので、この情報をVPN、SSLに使用することで、実施可能である。

【 0 0 6 9 】

図 2 5 では、保守センタ 1 0 1、開発センタ 1 0 5、コンピュータセンター 1 0 7、顧客管理センター 2 0 0 1、顧客オフィス 2 0 1 0 間をすべてインターネットで接続した場合のハードウェア接続図である。

【 0 0 7 0 】

コンピュータセンター内に顧客 Intranet 2 5 0 1 を配置し、DKC 1 1 0, 1 1 1, 1 1 2 及び RMC 1 0 8 を当該顧客 Intranet 2 5 0 1 にすべて接続する。インターネット 1 0 4 への接続方法は、当該顧客の Intranet の接続ポリシーにより様々な形態が考えられるのでここでは言及しない。例としては、常時接続型の専用 LAN としインターネット 1 0 4 と顧客 Intranet 2 5 0 1 との間を Firewall で保護する方法等がある。

【 0 0 7 1 】

この接続方法の場合、各 DKC に具備される SVP 9 1 0 は、図 9 で示す DKC 保守用 LAN 1 0 9 との I/F である DKC 保守 LAN I/F が、顧客 Intranet LAN I/F に変わる。また、RMC 1 0 8 は図 1 0 で示す DKC 保守 LAN I/F が、顧客 Intranet LAN I/F に変わり、また図 1 0 で示す 1 0 4 インターネットとの接続 I/F がなくなり、従来 1 0 4 インターネットとの間でやりとりしていた情報は、すべて顧客 Intranet 2 5 0 1 経由でインターネット 1 0 4 と接続される。これに伴い、SVP 9 1 0 及び RMC 1 0 8 のセキュリティを確保する必要が生じる。

【 0 0 7 2 】

図 2 6 は、SVP 9 1 0 が顧客 Intranet 2 5 0 1 と接続した場合のソフトウェア構成図である。SVP 9 1 0 は、8 1 3 DKC 内部 LAN と接続し、CHA、DKA とデータ通信可能となっている。2 6 0 1 障害監視は、CHA、DKA 等の障害発生を監視する。制御プログラムの交換も対象となる。2 6 0 2 保守センタ報告部は、障害監視 2 6 0 1 から伝達された障害情報（障害に限らず

一般保守情報も含む) が、保守用管理サーバ 1 0 2 へ伝達するために保守センタ通信部 2 6 0 3 へデータ転送する。保守センタ通信部 2 6 0 3 は、2 6 0 2 保守センタ報告部からのデータをセンタへ報告するための通信や、保守用管理サーバ 1 0 2 から指示のあったデータを受け取り、必要に応じて遠隔保守制御部 2 6 0 5 を起動する。保守センタ間セキュリティ 2 6 0 4 は、保守用管理サーバ 1 0 2 とのデータ送受信において、セキュリティ保護するためのロジックである。具体的には、外部からの接続要求に対するチェック、データ転送時の V P N 構築、または S S L による暗号化通信路の確立等を実施する、F i r e w a l l である。

【 0 0 7 3 】

遠隔保守制御部 2 6 0 5 は、保守用管理サーバ 1 0 2 より制御プログラムの交換指示があった場合に起動され、D K C ダウンロード制御部 2 0 5 またはプログラム更新制御部 2 0 2 を起動する。R M C 通信部 2 6 0 6 は、R M C 1 0 8 とのデータ送受信を実施するロジックである。R M C 間セキュリティ 2 6 0 7 は、R M C 1 0 8 とのデータ送受信におけるセキュリティ確保のためのロジックである。具体的には、保守センタ間セキュリティ 2 6 0 4 と同等の F i r e w a l l 機能を具備している。

【 0 0 7 4 】

図 2 7 は、セキュリティ機能を具備した R M C 1 0 8 のソフトウェア構成図である。F i r e w a l l 2 7 1 0 としては、S V P 間セキュリティ 2 7 0 3、センタ間セキュリティ 2 7 0 5 を具備する。S V P 間セキュリティ 2 7 0 3 は、S V P との通信を実施する上でのセキュリティ確保のためのロジックである。センタ間セキュリティ 2 7 0 5 は、制御プログラム配信サーバ 1 0 6 との通信を実施する上でのセキュリティ確保のためのロジックである。また、R M C ダウンロード制御部 3 0 1 は、S V P 通信部 2 7 0 2、保守センタ通信部 2 7 0 4 と I / F を有し、データ通信処理を実現する。また、S V P 9 1 0 と保守用管理サーバとのゲートウェイ接続可能とするために、保守情報中継 2 7 0 1 を具備し、S V P 通信部 2 7 0 2 と保守センタ通信部 2 7 0 4 とのデータ送受信の橋渡しを実現する。

【 0 0 7 5 】

以上、本発明の一実施形態を説明したが、本発明はこれに限定されず、特許請求の範囲の要旨を逸脱しない範囲で種々の変更が可能であることは云うまでもない。

【 0 0 7 6 】

【発明の効果】

以上の説明から明らかなように、本発明によれば、既に設置されているインターネットを使用することで、制御プログラム転送に要する時間が削減でき、また複数コンピュータセンター同時転送も可能となる。また、制御プログラム更新指示、認証情報は保守センターから公衆回線経由で直接コンピュータセンターへ送信することで、第三者による故意の制御プログラム更新を防ぐことができる。

【図面の簡単な説明】

【図 1】

本発明の制御プログラム自動更新方式を適用したシステムの一実施形態の構成を示すブロック図である。

【図 2】

ディスク制御装置の制御プログラム更新方式に関連する構成図である。

【図 3】

リモートコンソールの制御プログラム更新方式に関連する構成図である。

【図 4】

制御プログラムの自動配信と自動更新の連続実行指示を行った場合の処理動作を示すシーケンス図である。

【図 5】

制御プログラムの自動配信のみを実行する場合のシーケンス図である。

【図 6】

制御プログラムの自動更新のみを実行する場合のシーケンス図である。

【図 7】

従来の制御プログラム自動更新方式を適用したシステムの構成を示すブロック図である。

【図 8】

DKC 1 1 0 の内部構造を示したハードウェア構成図である。

【図 9】

SVP 9 1 0 の内部構造を示したハードウェア構成図である。

【図 1 0】

RMC 1 0 8 の内部構造を示したハードウェア構成図である。

【図 1 1】

第 1 の実施例で示す各センタ間のデータの流れを示したデータフロー図である。

【図 1 2】

保守管理サーバ 1 0 2 上で表示する更新指示画面の出力例を示した説明図である。

【図 1 3】

データ 1 0 1 1 のデータフォーマット図である。

【図 1 4】

保守管理サーバが SVP に対して転送するデータ 1 0 1 2 のデータフォーマット図である。

【図 1 5】

DKC 1 1 0 の SVP から RMC 1 0 8 に対して送信する 1 0 1 3 のデータフォーマット図である。

【図 1 6】

交換処理結果 1 0 1 7 を受け取った保守管理サーバが表示する更新結果一覧画面を示した説明図である。

【図 1 7】

保守管理サーバから、現在の DKC の更新状態を取得した結果を表示した説明図である。

【図 1 8】

第 2 の実施例を実施するデータフロー図である。

【図19】

制御プログラム配信サーバ106で実施するソフトウェア構成図である。

【図20】

顧客が更新要求を発行する場合のデータフロー図である。

【図21】

保守センタ101とコンピュータセンタ107との間を、公衆回線網103でTCP/IPのネットワークとして接続したときのハードウェア接続構成図である。

【図22】

データ2003のデータフォーマット図である。

【図23】

要求入力2011のソフトウェア構成図である。

【図24】

顧客情報管理サーバ2002のソフトウェア構成図である。

【図25】

保守センタ101、開発センタ105、コンピュータセンター107、顧客管理センター2001、顧客オフィス2010間をすべてインターネットで接続した場合のハードウェア接続図である。

【図26】

SVP910が顧客Intranet2501と接続した場合のソフトウェア構成図である。

【図27】

セキュリティ機能を具備したRMC108のソフトウェア構成図である。

【符号の説明】

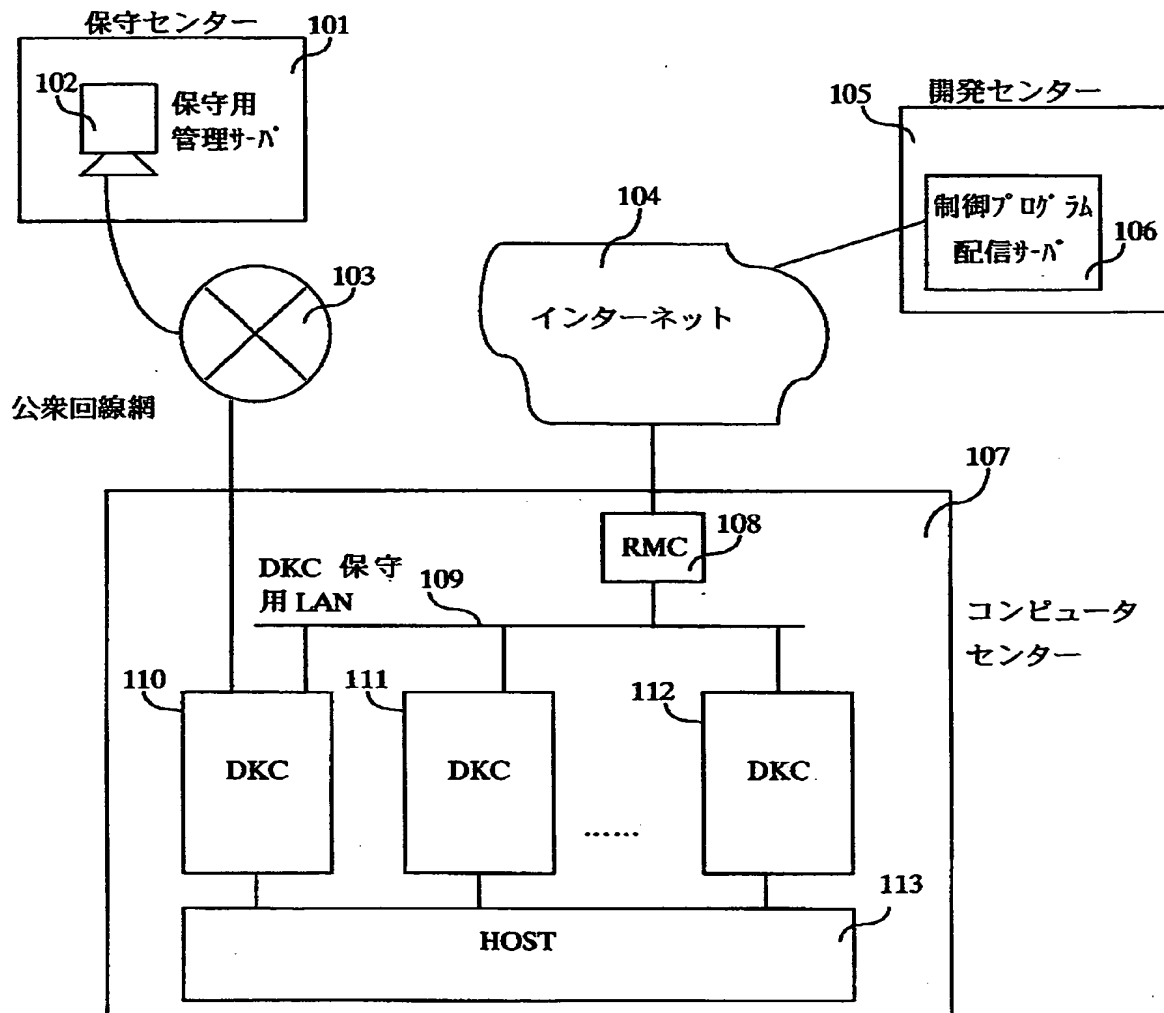
101…保守センター、102…保守用管理サーバ、103…公衆回線網、
104…インターネット、105…開発センター、106…制御プログラム
配信サーバ、107…コンピュータセンター、108…リモートコンソール、
109…ローカルエリアネットワーク、110、111、112…ディスク制
御装置、201…保守センター通信部、202…プログラム更新制御部、20

3、204…プロセッサ、205…ディスク制御装置ダウンロード制御部、206…ディスク制御装置プログラム格納部、301…リモートコンソールダウンロード制御部、302…リモートコンソールプログラム格納部、

【書類名】 図面

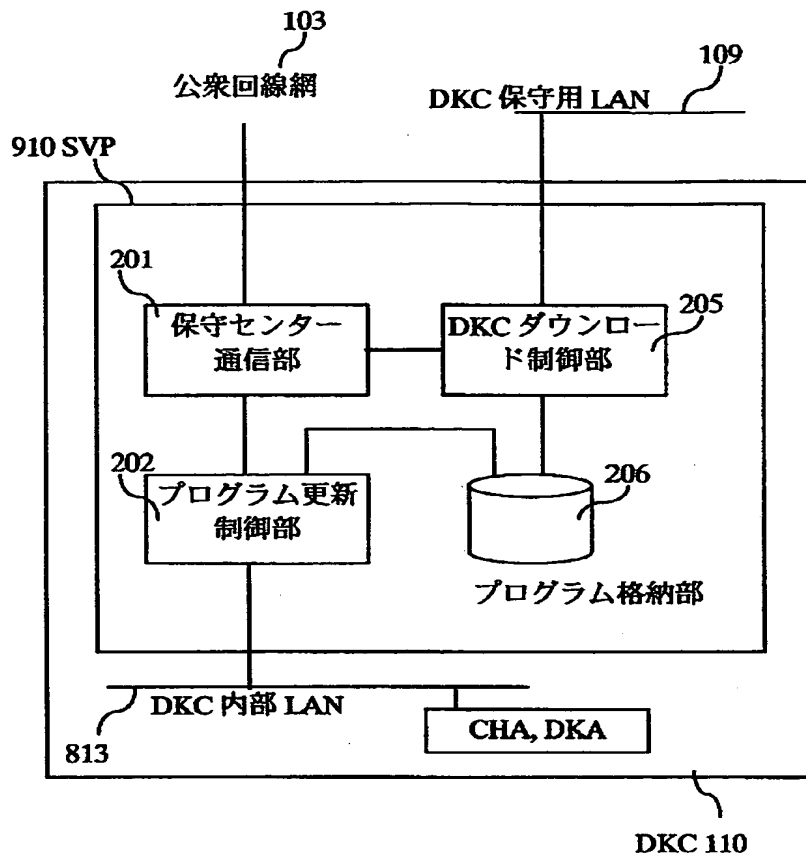
【図 1】

図 1



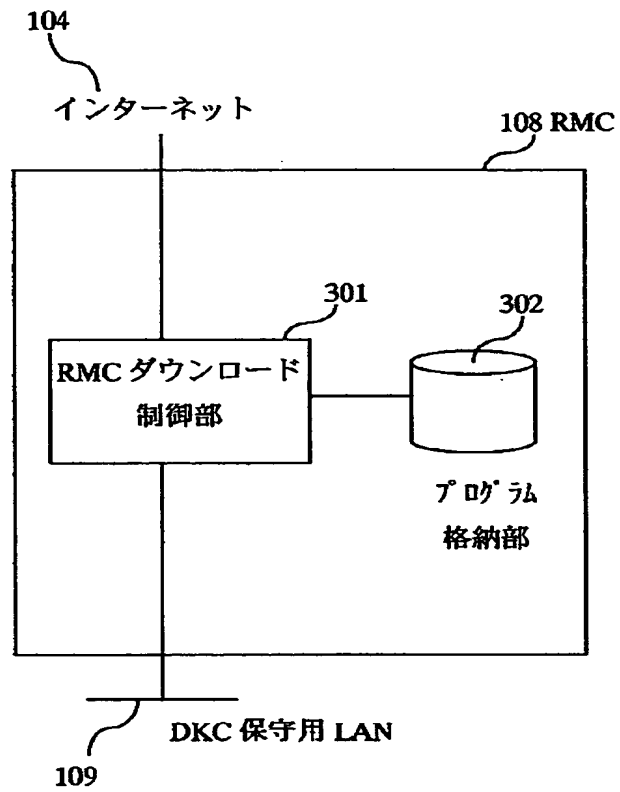
【図 2】

図 2



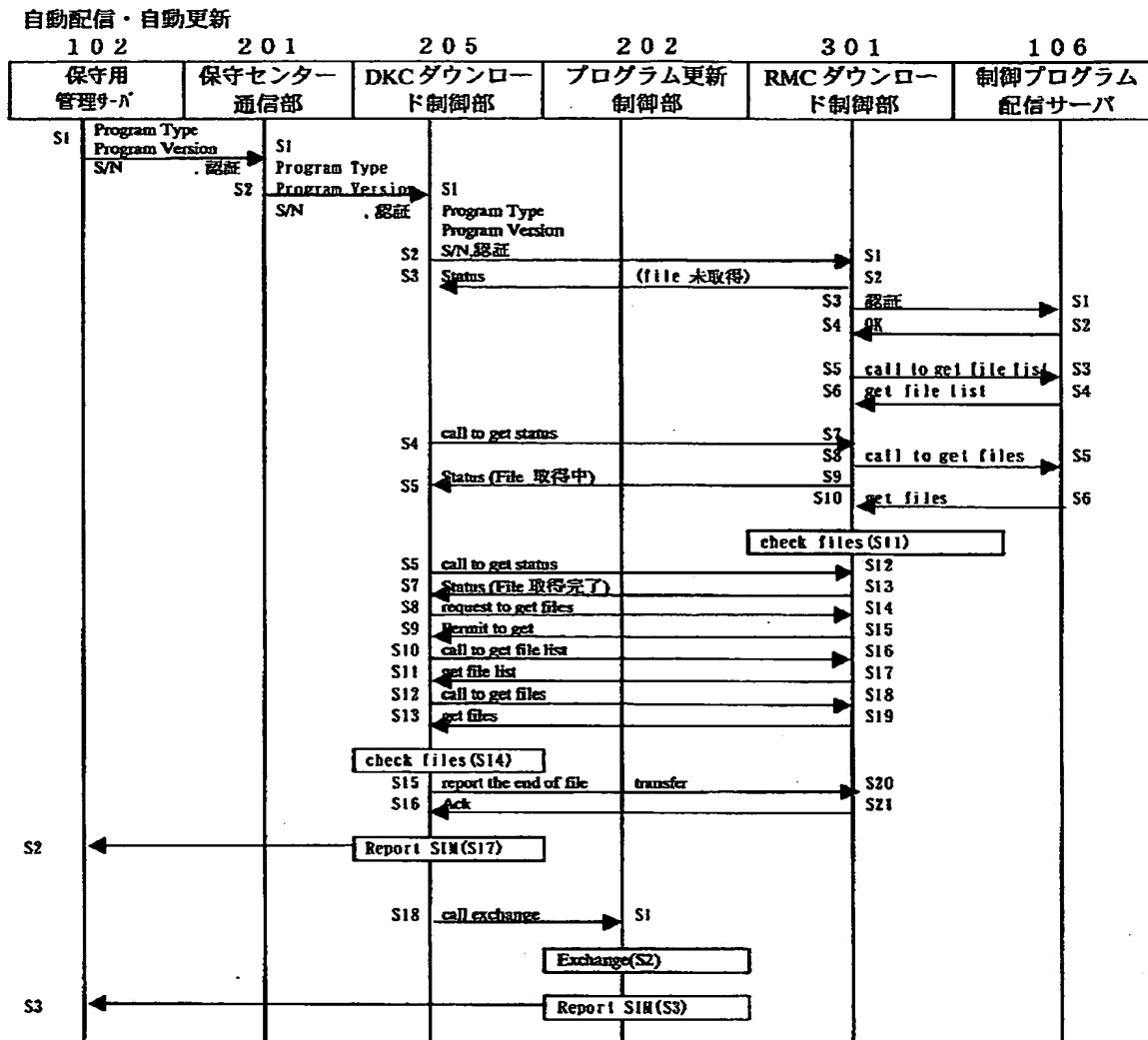
【図 3】

図 3



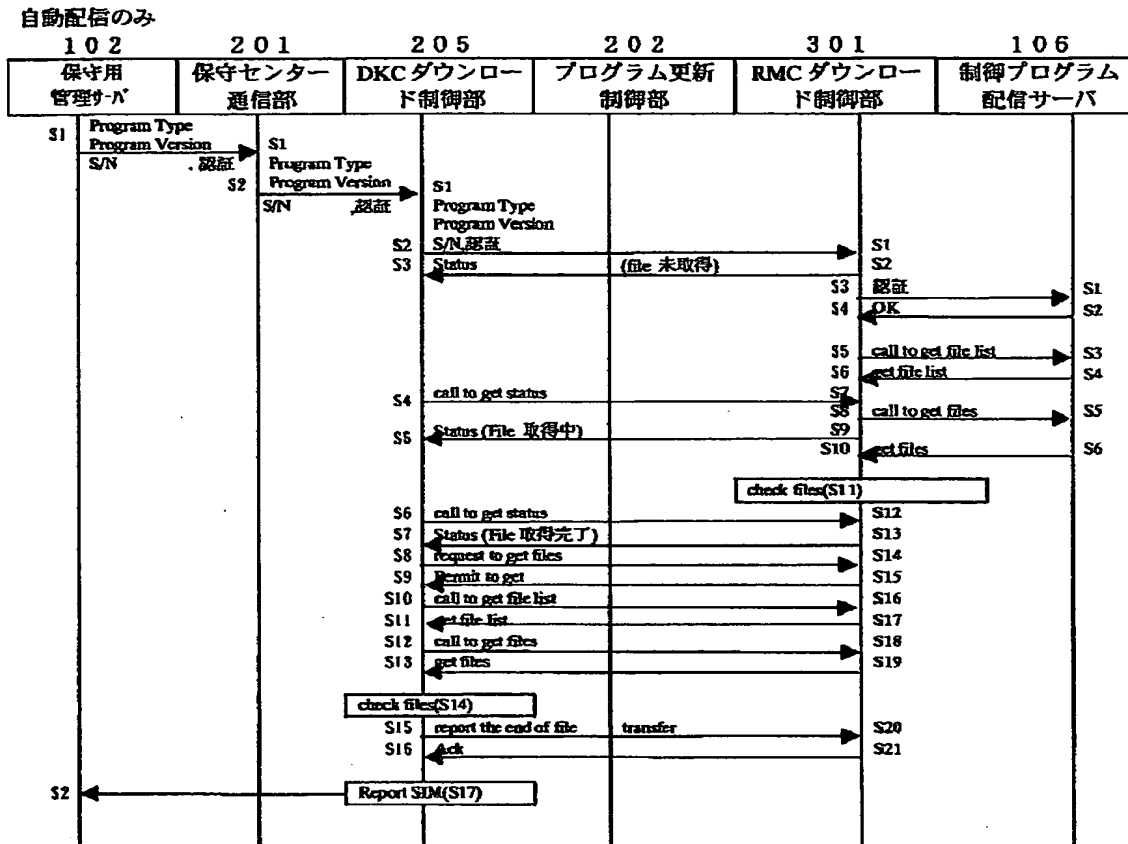
【図 4】

図 4



【図 5】

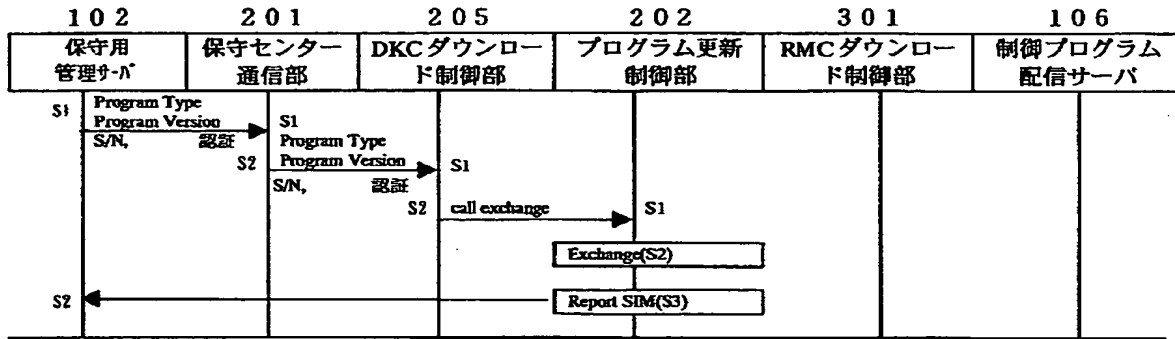
図 5



【図 6】

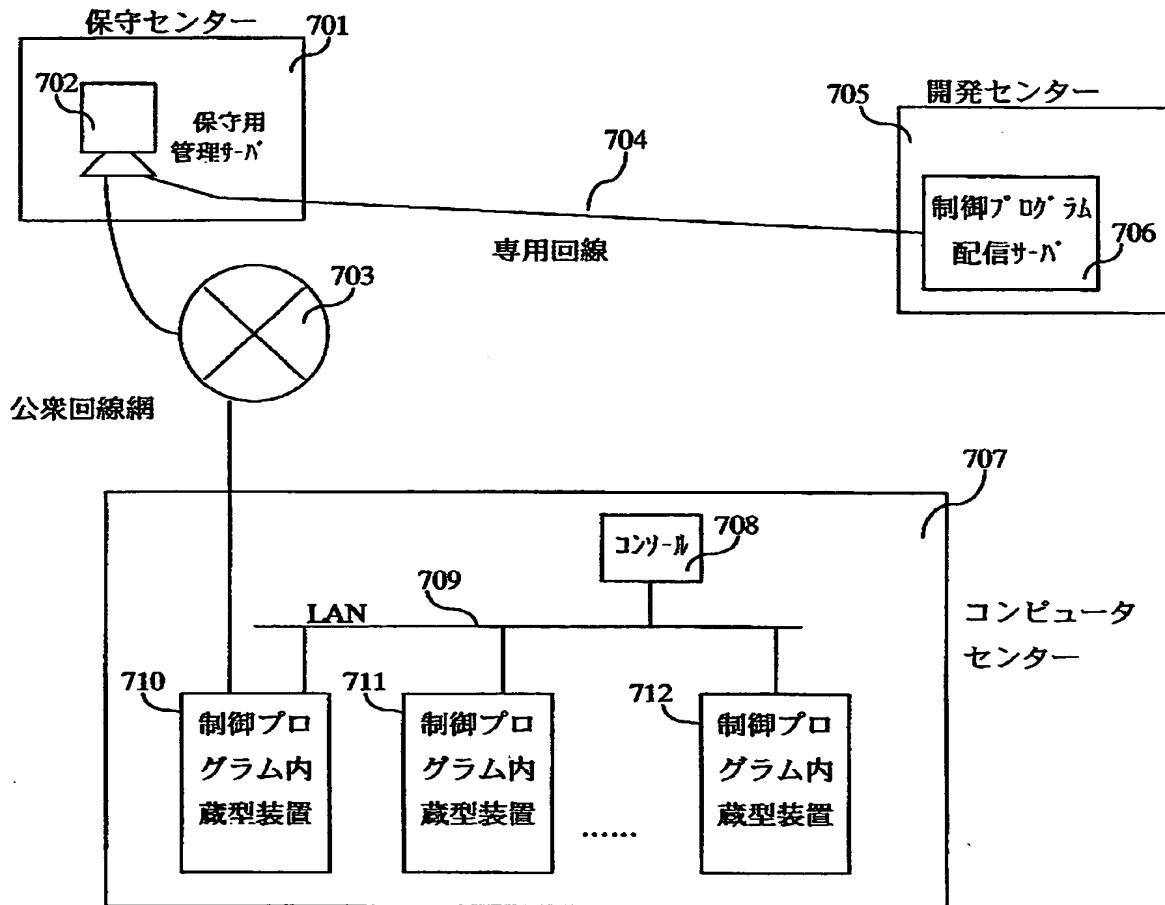
図 6

自動更新のみ



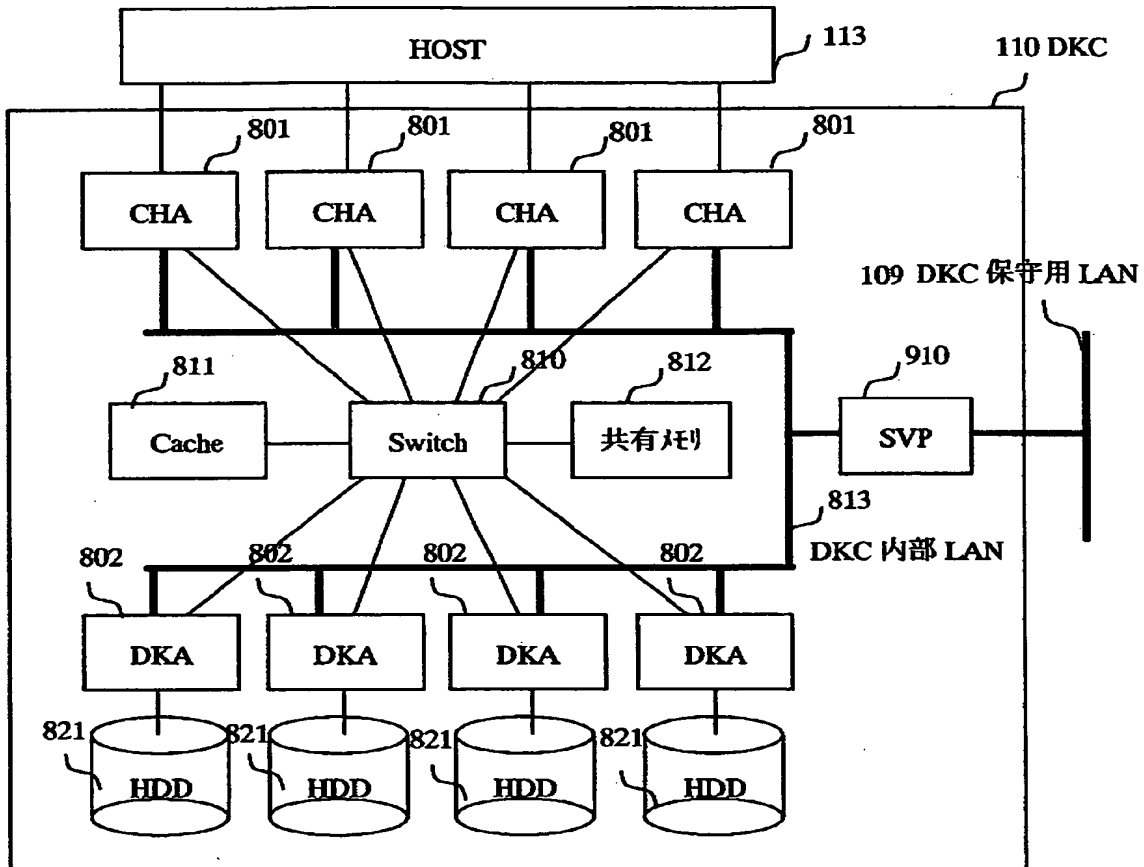
【図 7】

図 7



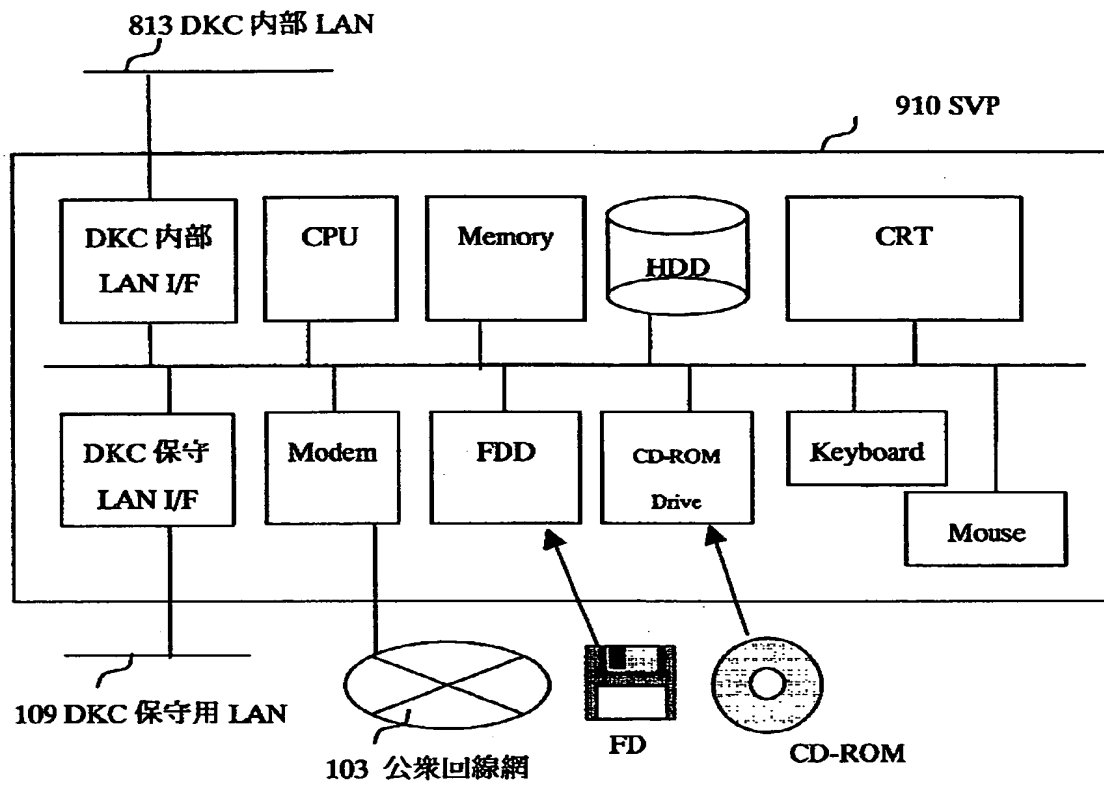
【図8】

図8



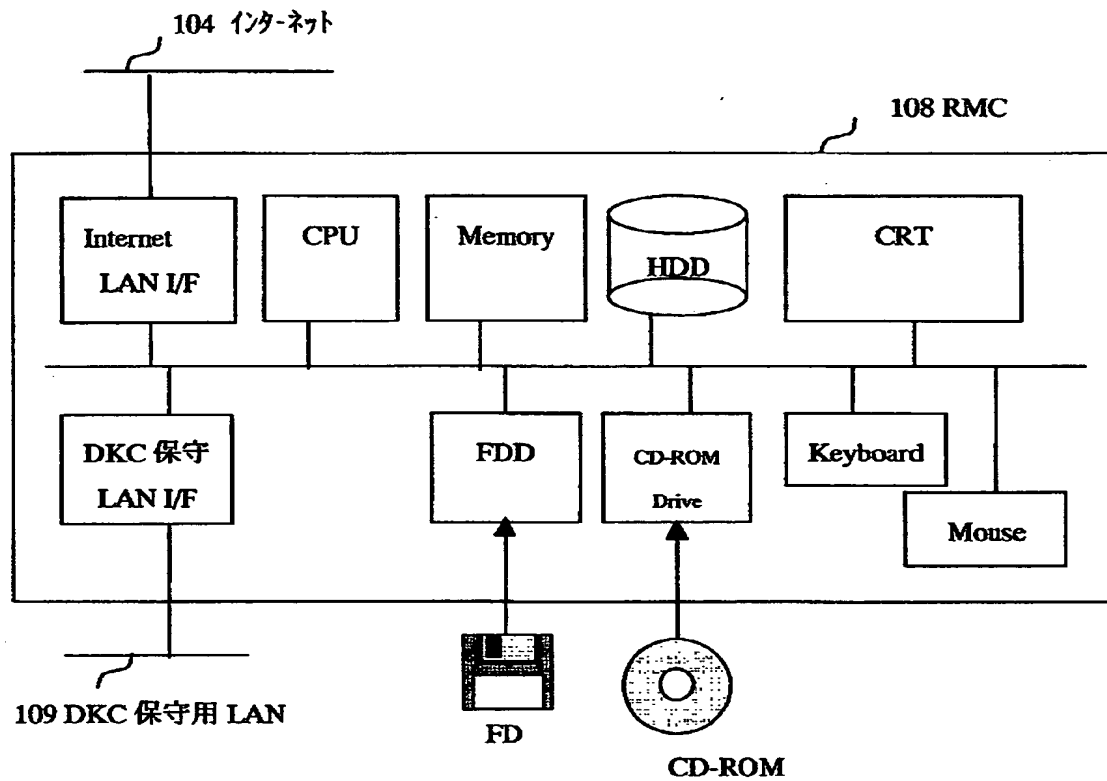
【図 9】

図 9



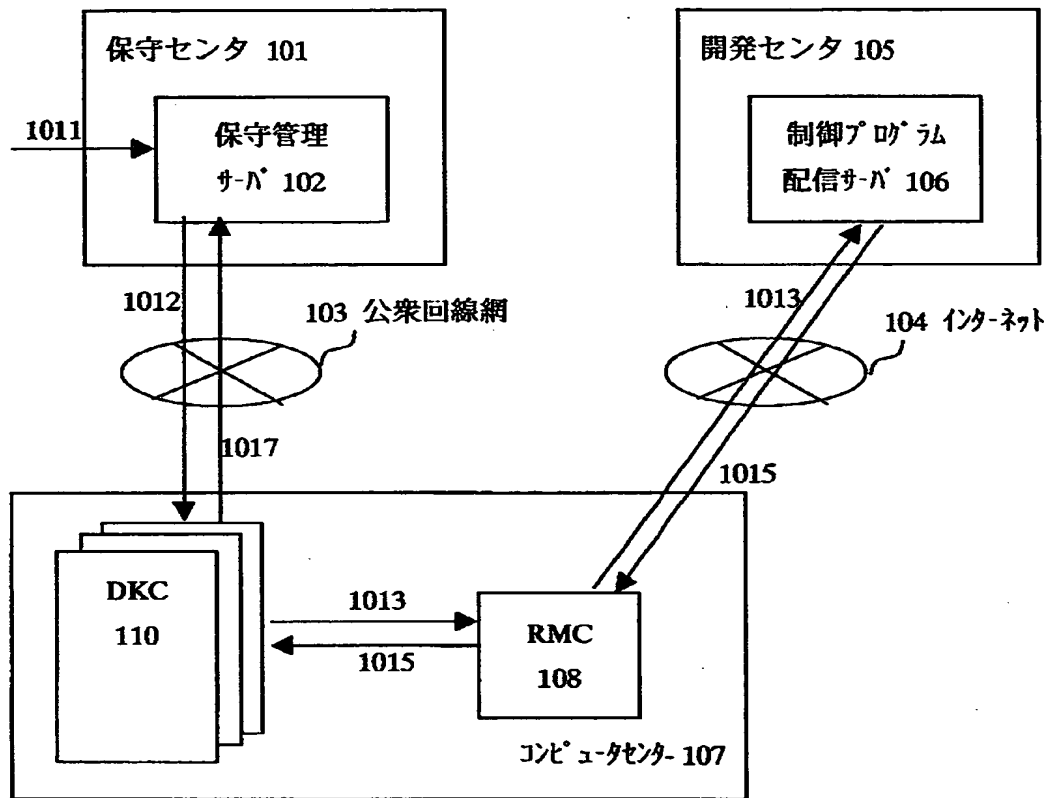
【図 1 0】

図 10



【図 11】

図 11



【図 1 2】

図 12

更新指示画面

Type	S/N	Version	更新モード
H-65A1-1	30051	01-02-35-67/00	Download & Update
H-65A1-1	30052	01-02-35-67/00	Download
H-65A1-1	30053	01-02-35-67/00	Update

更新 キャンセル

入力 Field

【図 1 3】

図 13

1011

H-65A1-1	製品型式(Type)
30051	製品製造番号(S/N)
01-12-35-67/00	制御プログラムバージョン
Download & Update	更新モード

【図 14】

図 14

1012

H-65A1-1	製品型式(Type)
30051	製品製造番号(S/N)
01-12-35-67/00	制御プログラムバージョン
Download & Update	更新モード
HSVPMaintain	SVP 認証キー (ログイン・パスワード)
H30051svp9z	
H30051MDFYX	配信サーバ認証キー (ログイン・パスワード)
Tsh27ymK	
ftp://strProg.hitachi.co.jp/pub/DKC/H65A1-1/01-02/3567.zip	ファイルロケーション

【図 15】


図 15

1013

H-65A1-1	製品型式(Type)
30051	製品製造番号(S/N)
01-12-35-67/00	制御プログラムバージョン
Download & Update	更新モード
H30051MDFYX	配信サーバ認証キー (ログイン・パスワード)
Tsh27ymK	
ftp://strProg.hitachi.co.jp/pub/DKC/H65A1-1/01-02/3567.zip	ファイルロケーション

【図 1 6】

図 16

更新結果一覧				
Type	S/N	Version	更新結果	
H-65A1-1	30051	01-02-35-67/00	正常終了	
H-65A1-1	30052	01-02-35-67/00	異常終了(79F4)	
H-65A1-1	30053	01-02-35-67/00	正常終了(転送)	
				閉じる

【図 1 7】

図 17

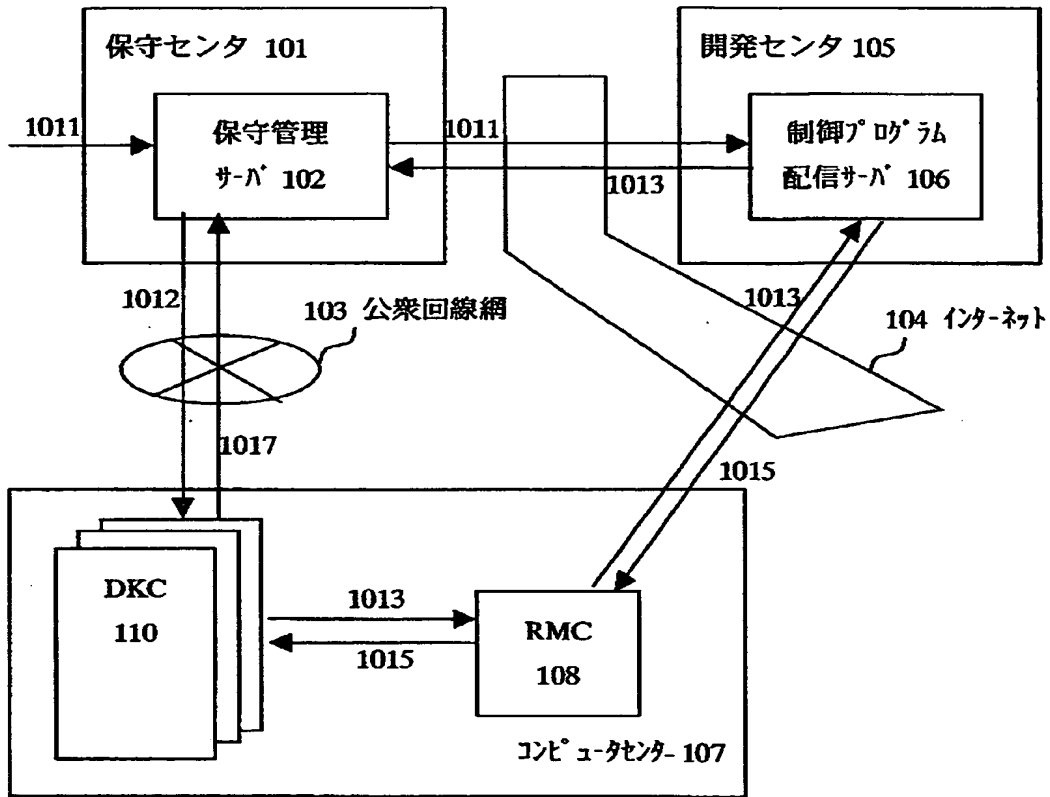
装置更新状態一覧

Type	S/N	現行 Version	更新結果	配信済 Version
H-65A1-1	30051	01-02-35-67/00		未配信
H-65A1-1	30052	01-01-89-24/00	配信済(未交換)	01-02-35-67/00
H-65A1-1	30053	01-01-89-24/00	配信済(未交換)	01-02-35-67/00

閉じる

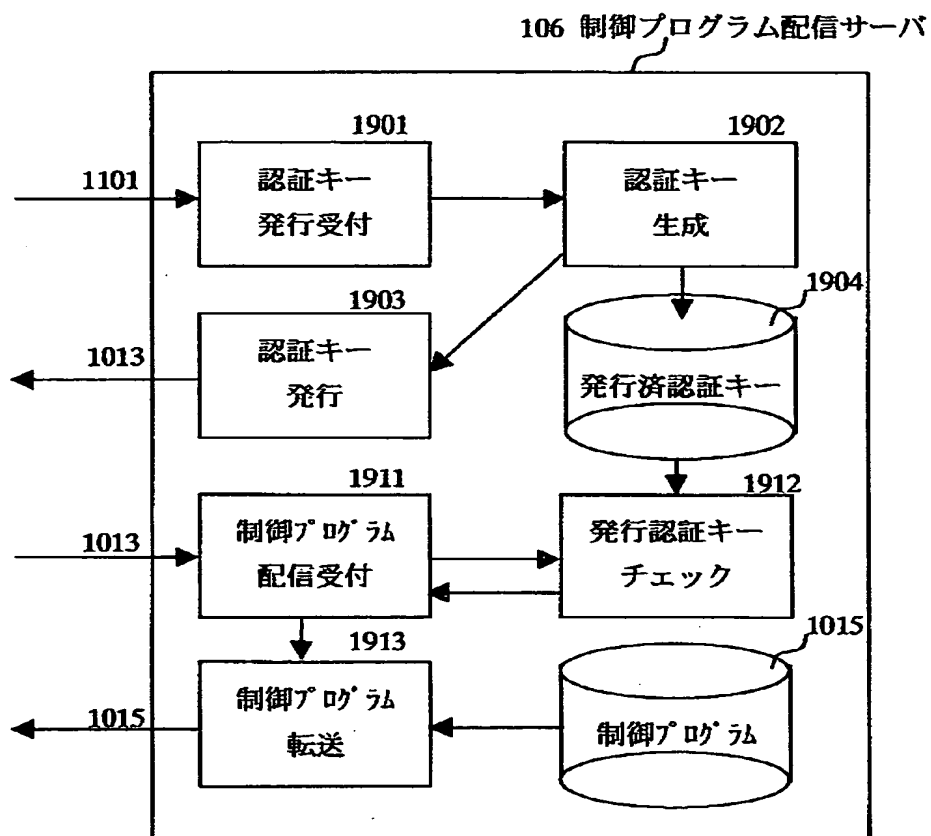
【図 1 8】

図 18



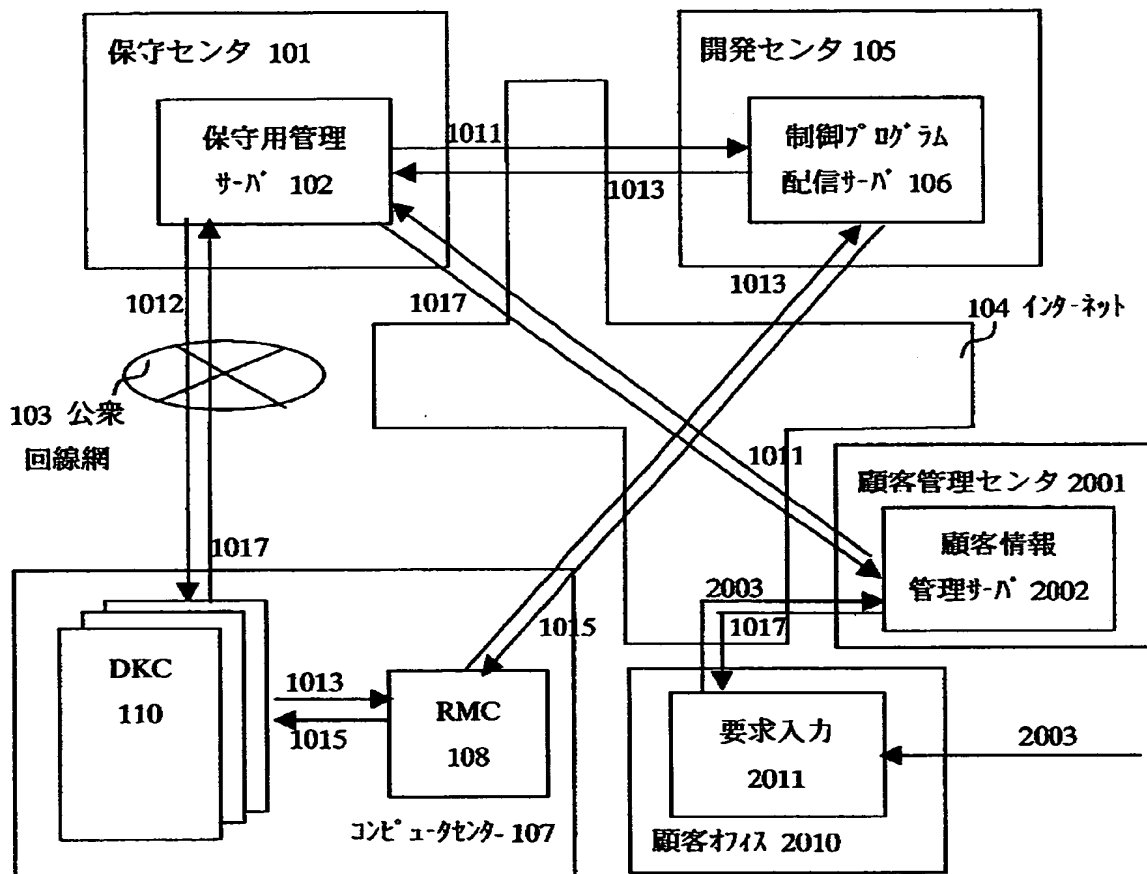
【図 1 9】

図 19



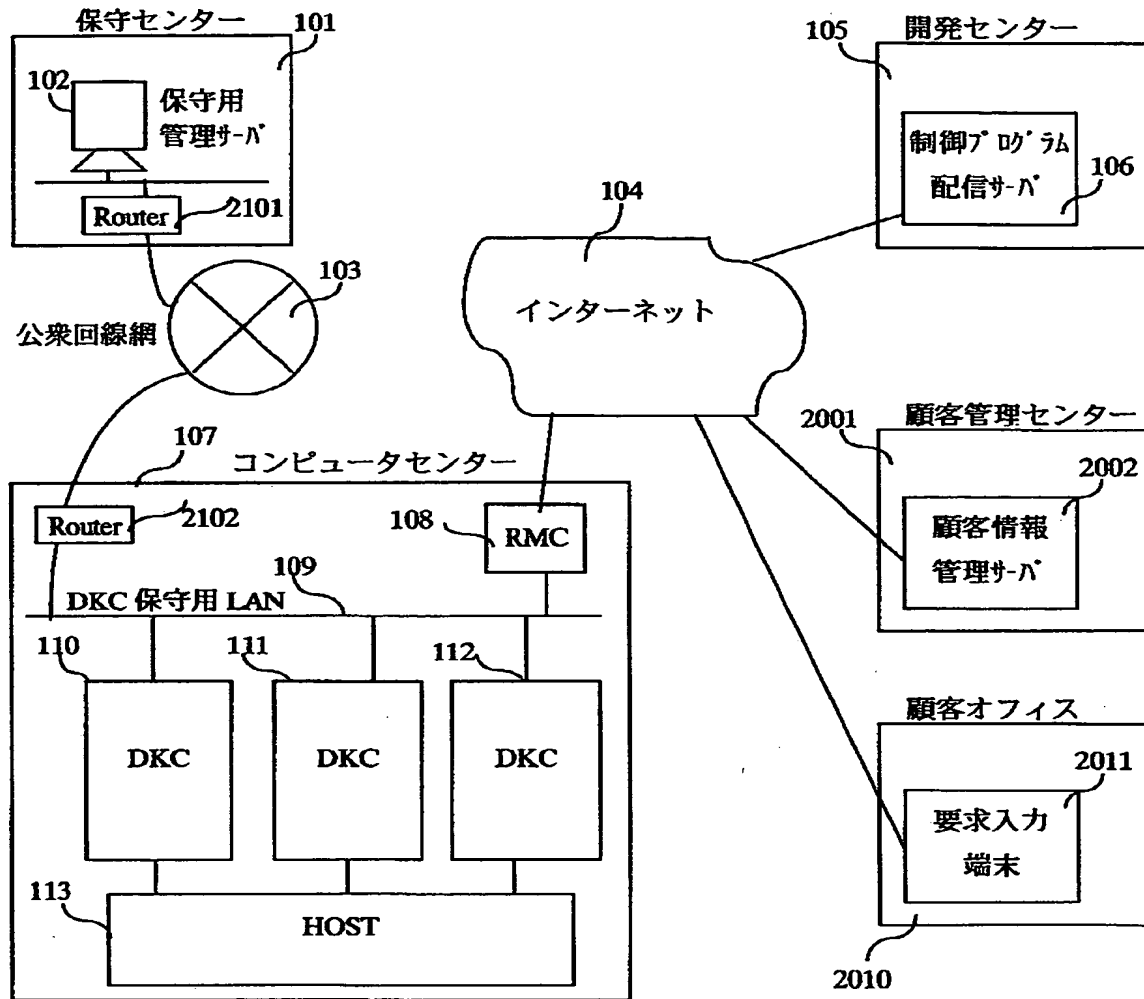
【図 20】

図 20



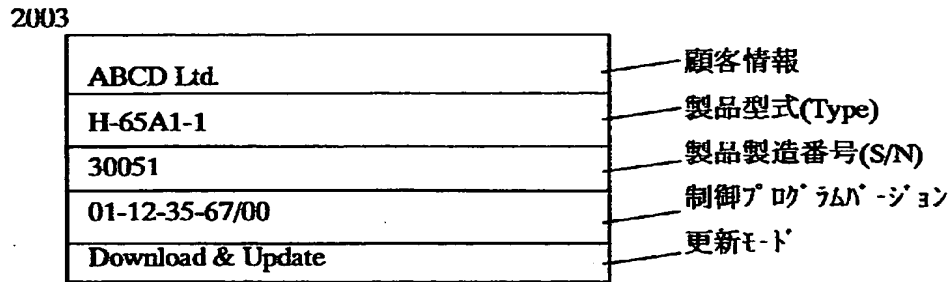
【図 21】

図 21



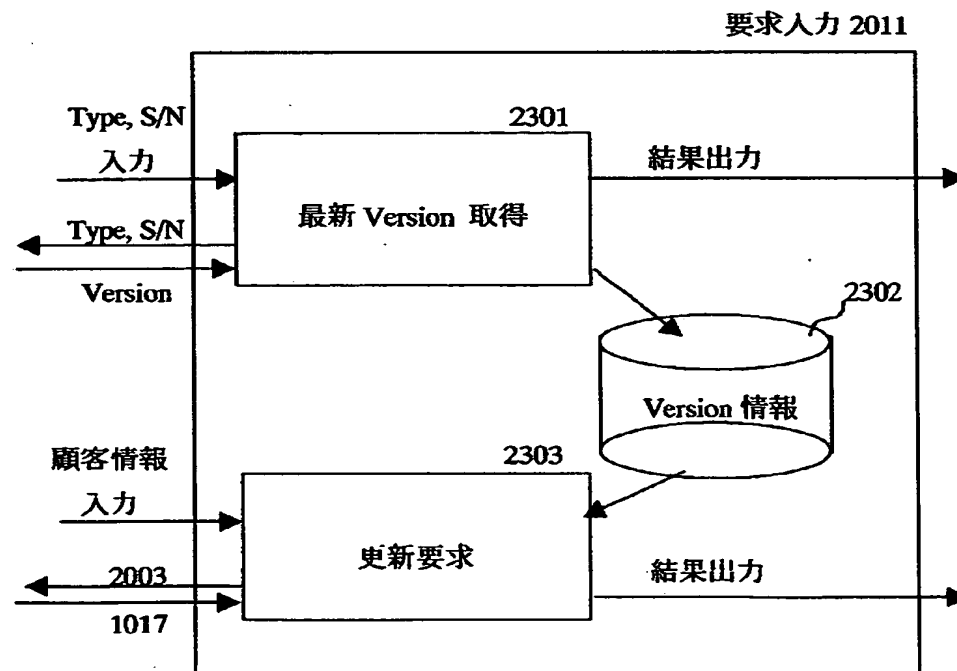
【図 2 2】

図 22



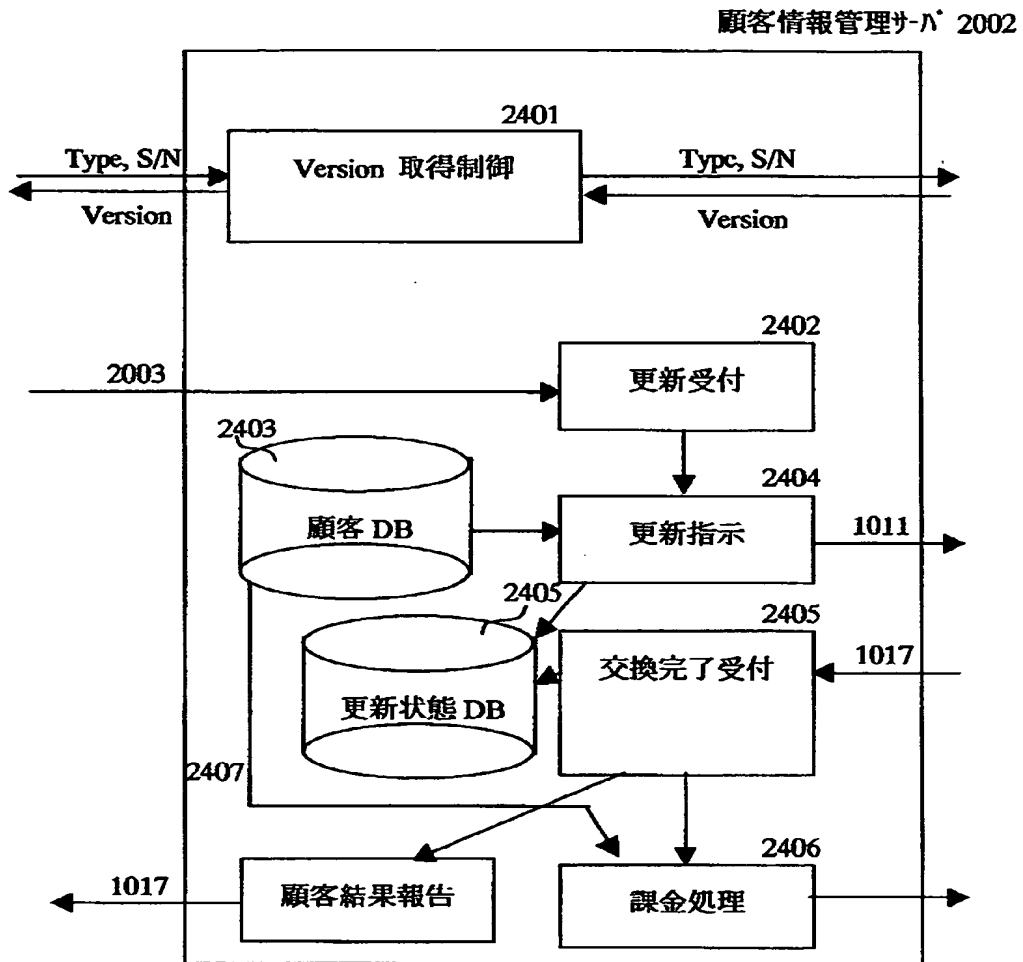
【図 2 3】

図 23



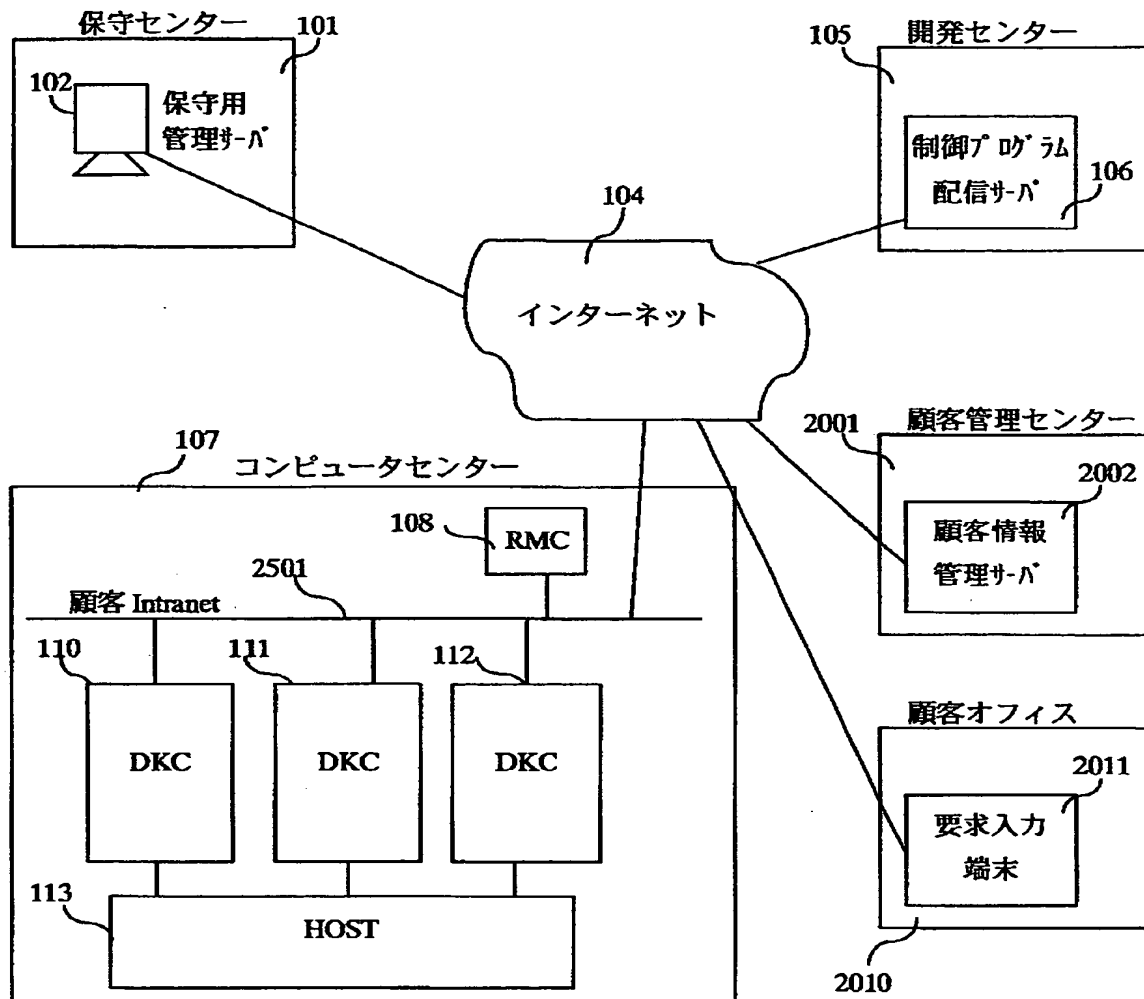
【図 2 4】

図 24



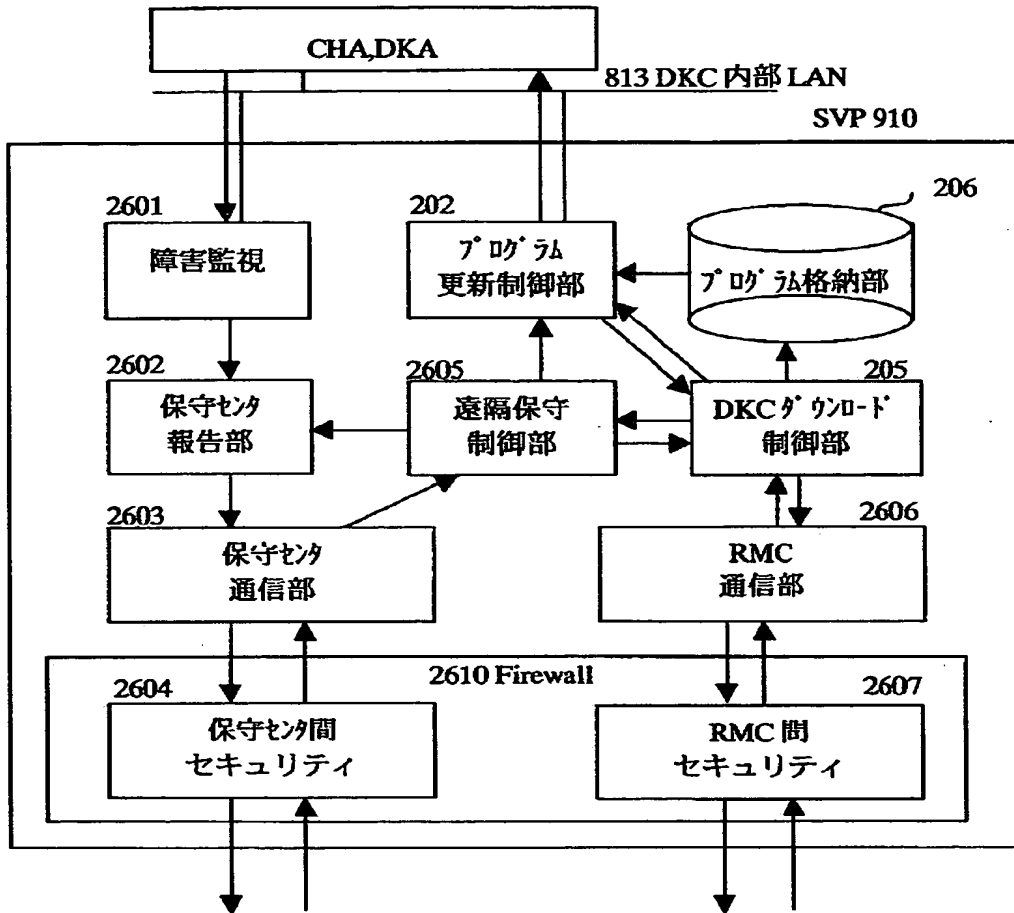
【図 25】

図 25



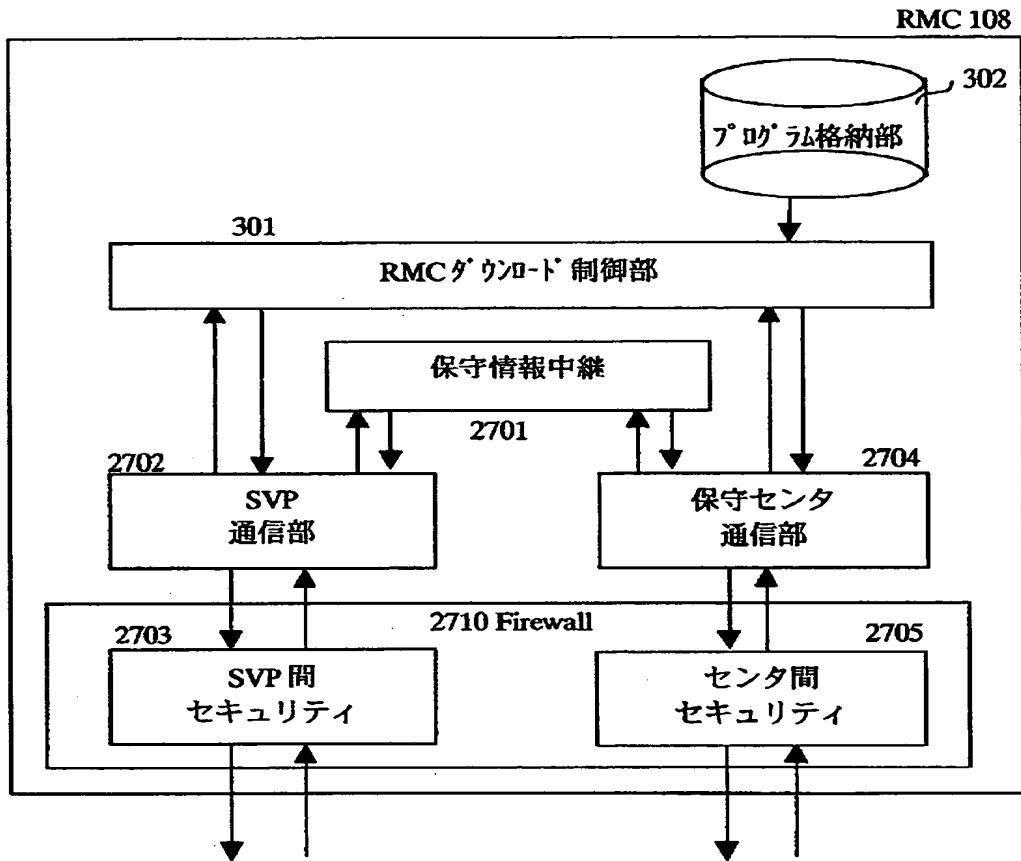
【図 2 6】

図 26



【図 2 7】

図 27



【書類名】 要約書

【要約】

【課題】

安全性を高めるため、制御プログラムの更新指示はインターネットを使用しないで、制御プログラムにのダウンロード処理にのみインターネットを使用することが課題である。

【解決手段】

保守センター101に設置されている保守用管理サーバ102から制御プログラムの配信と更新の指示が公衆回線網103を経由してDKC110に行われる。指示を受け取ったDKC110はRMC108に対して制御プログラム配信サーバ106からの制御プログラムダウンロードの指示を行う。RMC108はインターネット104を経由して制御プログラム配信サーバ106から制御プログラムのダウンロードを実施する。ダウンロードされた制御プログラムは一旦RMC108内に格納された後、DKC110、111、112へ転送され、DKC内部で更新処理が実行される。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地

氏 名 株式会社日立製作所

出 願 人 履 歴 情 報

識別番号 [0 0 0 2 3 3 0 5 5]

1. 変更年月日 1 9 9 0 年 8 月 7 日

[変更理由] 新規登録

住 所 神奈川県横浜市中区尾上町 6 丁目 8 1 番地

氏 名 日立ソフトウェアエンジニアリング株式会社